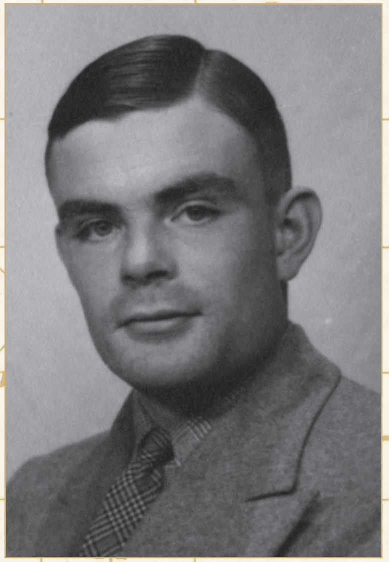


Michael Ventris (left, courtesy of the Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge) and Alan Turing (right, reproduced by kind permission of King's College Library, Cambridge, AMT/K/7/9)

Secret texts and secret writing have an age-old fascination. In this book two stories are told: of the people who worked on breaking vital codes in the Second World War and those who deciphered the Linear B script - Europe's earliest comprehensible writing system. Here experts in the fields of Mycenaean epigraphy and the study of the Aegean Bronze Age join with fellow specialists in mathematics, cryptography and the history of computer. They show how collaboration between people with a wide range of expertise in disparate fields can result in great discoveries, whether they are mathematicians or linguists, or just good at puzzles! Both groups of pioneer codebreakers needed original thinkers and the stories of those involved, especially Alan Turing and Dillwyn Knox at Bletchley Park and Michael Ventris and John Chadwick in Cambridge, are told here.

The
Fitzwilliam
Museum
CAMBRIDGE

Front cover illustrations: left, clay tablet from Knossos (Courtesy of the Ashmolean Museum, University of Oxford) right, Enigma machine rotors (Image provided by The Enigma Project) Backgrounds: front cover from a letter of Alan Turing to his mother (Courtesy of King's College Library, Cambridge), back cover, from Ventris's Work Note 17 (Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)

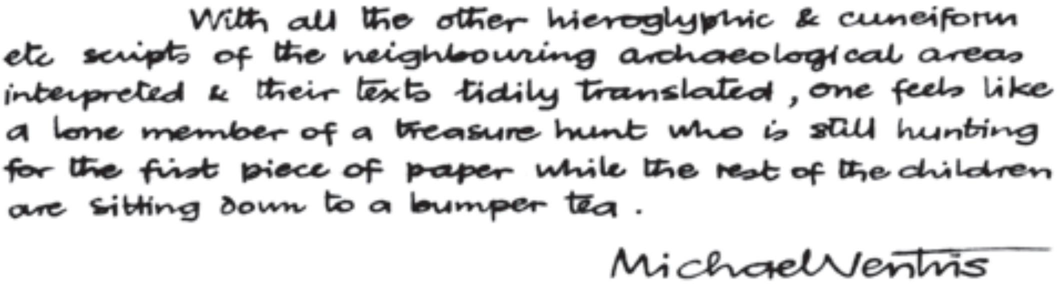
ISBN 978-1-910731-09-3
9 781910 731093

Codebreakers and Groundbreakers ed. Galanakis, Christophilopoulou and Grime The Fitzwilliam Museum

Codebreakers and Groundbreakers

edited by
Yannis Galanakis, Anastasia Christophilopoulou
and James Grime

Codebreakers and Groundbreakers



With all the other hieroglyphic & cuneiform etc scripts of the neighbouring archaeological areas interpreted & their texts tidily translated, one feels like a lone member of a treasure hunt who is still hunting for the first piece of paper while the rest of the children are sitting down to a bumper tea.

Michael Ventris

Extract from a letter from Michael Ventris to Stuart Piggott in Oxford, 21 September 1953. Courtesy of the Institute of Archaeology, University of Oxford.

Codebreakers and Groundbreakers
First published in 2017
by The Fitzwilliam Museum
Trumpington Street
Cambridge, CB1 2RB
www.fitzmuseum.cam.ac.uk

Designed and typeset by Palindrome
Printed in England by Charlesworth Press

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-1-910731-09-3

Codebreakers and Groundbreakers

edited by

Yannis Galanakis, Anastasia Christophilopoulou and James Grime

The
Fitzwilliam
Museum
CAMBRIDGE

Contents

Part 1 The Decipherment of Linear B

Part 2 The Second World War: Computers and the Future

Foreword

Tim Knox

On 1 July 1952 Michael Ventris, an architect by training who had turned linguist, announced on BBC radio his proposed decipherment of the Linear B script, a script that had puzzled many scholars, for over fifty years. The decipherment of the Linear B script, which was preserved by accident in a number of clay baked tablets, excavated firstly at Knossos and later at a number of other Mycenaean sites, changed for ever our understanding of the Late Bronze Age world and eventually our approach to the study of ancient Greece.

A little more than a year earlier, on 15 May 1951, mathematician Alan Turing (1912–54) argued, during a BBC Third Programme broadcast, that 'It is now not altogether unreasonable to describe digital computers as brains.' This broadcast had followed the publication of an important paper, in which Turing had speculated about the possibility of creating machines that think. Turing became well known posthumously as the most influential codebreaker of the Second World War, but his reputation goes beyond his work at Bletchley Park and the breaking of the Enigma. Many mathematicians and computers scientists today credit him with the very first definition of artificial intelligence and in general his work in fields such as computing and biology means Turing is considered one of the twentieth century's greatest mathematicians.

These two stories, the decipherment of an Aegean Bronze Age script and the efforts of the British codebreakers during the Second World War, brought together and explained in the exhibition and this book, *Codebreakers and Groundbreakers*, interlink and engage with two distinct – yet relevant – narratives. Since the declassification of the codebreaking efforts of the Second World War, the story of Bletchley Park has become well known. Turing was undoubtedly the most famous of the codebreakers but the teams working together included experts of many other non-scientific disciplines, such as linguists John Tilan or Dilwyn 'Dilly' Knox, who collaborated with the mathematicians under the spirit of a truly interdisciplinary atmosphere. The exhibition, an unusual one for the Fitzwilliam Museum, arose from extensive research into the biographies and associated material and archival evidence left behind by this diverse group of Second World War British codebreakers.

Two particular historical accounts capture perfectly the importance of the codebreakers' work whether in breaking a code or in solving the riddle of an ancient script. The first account comes to us from Hugh Alexander, Turing's deputy in Hut 8. Speaking about Turing's contribution he has said,

> There should be no question in anyone's mind that Turing's work was the biggest factor in Hut 8's success. . . . It is always difficult to say that anyone is 'absolutely indispensable', but if anyone was indispensable to Hut 8, it was Turing . . . many of us in Hut 8 felt that the magnitude of Turing's contribution was never fully realised by the outside world.

A second account, perfectly describing the challenge as well as the frustration of the decipherer himself, is preserved in one of Michael Ventris's own letters to Stuart Piggott in Oxford, shortly after the decipherment of the Linear B script.

> With all the other hieroglyphic and cuneiform etc scripts of the neighbouring archaeological areas interpreted and their texts tidily translated, one feels like a lone member of a treasure hunt who is still hunting for the first piece of paper while the rest of the children are sitting down to a bumper tea.

Codebreakers and Groundbreakers aimed to include only a few objects familiar from our collections in the Fitzwilliam or the Museum of Classical Archaeology. The aim was rather to show material from archives and collections that normally either require special permission to be viewed (such as the collection cypher machines including Enigma at the Government's Communication Headquarters, GCHQ), or ones usually accessed only by researchers in particular fields (such as the Turing archive held in King's College Cambridge or the Sir Arthur Evans and the Sir John Myres Archives held by the Department of Antiquities of the Ashmolean Museum). The amazing skills shared by the codebreakers and those who deciphered ancient scripts can thus be considered together. The unique objects displayed provide a refreshing view into the themes not usually explored by our audiences in our temporary exhibitions in the Fitzwilliam, as well as an important challenge for our curators to explore ideas and themes beyond their main expertise. The exhibition was curated, and this book edited, by Anastasia Christophilopoulou, Yannis Galanakis and James Grime, who have all contributed equally to bring the project to fruition.

We hope that this spirit of interdisciplinarity and exchange of ideas manifested in this exhibition, as well as in the composition of the research team who brought this idea to the Fitzwilliam, will continue to be celebrated in future research and exhibition projects between the University of Cambridge Museums and other University departments. Above all, it is hoped that *Codebreakers and Groundbreakers* will enthuse and engage our audiences with the exciting and complex interaction between the humanities and science.

Preface

A. Christophilopoulou

Codebreakers and Groundbreakers is an interdisciplinary exhibition project based on the history of cryptography. Cryptography is often referred to as a battle of intelligence between the 'codemakers' and the 'codebreakers', ancient or modern. However, it is also concerned with languages, mathematics and technology. This exhibition aspired to bring 'back to life' the people who broke the codes: those involved in breaking the Second World War codes and those who, working at the same time as the first group but independently from it, deciphered the Linear B script – Europe's earliest comprehensible writing system. Both groups of pioneer codebreakers were strongly connected to the University of Cambridge during the inter-war period and until the end of the 1950s.

This book reflects the dual character of the exhibition and intends to enrich the exhibition's narratives as well as reveal further aspects of the work and the times of the codebreakers. It contains essays by experts in the fields of Mycenaean epigraphy and the study of the Aegean Bronze Age (part 1, The Decipherment of Linear B), as well as in the fields of mathematics, cryptography and the history of computer science (part 2, The Second World War: Computers and the Future). A handlist of all objects and archival material displayed in the exhibition is presented at the end of the volume.

The story begins with the fascinating era of the discovery and naming of the Linear B script by Sir Arthur Evans, pioneer of the archaeology of prehistoric Crete and excavator of Knossos, providing insights into Evans's first ideas on the newly discovered hoard of clay documents. Then follows a concise analysis of the decipherment's process and the challenges involved in it, where particular tribute is paid to the 'unsung heroes' of the decipherment. The archaeological data, revealing associations between texts written in Linear B, as well as reconstructing the wider material world, is then explored. In chapter 4 Linear B is explained as one of a series of related writing systems, closely linked with two earlier scripts in use in Crete during the Middle and Late Bronze Ages, and more distantly related with the Late Bronze Age and Iron Age Cypriot syllabic systems. The special relationship between bright scientists and linguists, or other classicists all working as cryptanalysts is revealed in a chapter debating the composition of staff recruited by the Government Code and Cipher School (GC&CS, the forerunner of GCHQ) and within that the contribution of non-scientists. Finally, a chapter explaining the use of modern computing tools and methods in the study of antiquity as well as the new possibilities these methods offer in the reconstruction of past cultures and the process of deciphering ancient languages and scripts is provided.

The second part of this volume concerns itself with the birth of modern cryptography as the discipline was formulated in the context of the First and Second World Wars and how it later evolved to cover all aspects of the deep theory and widespread practice of coding and decoding information. This section of the book opens with an introduction delineating the connections between codebreaking and the dawn of early computer science, followed by a detailed account of Turing's contributions to Bletchley Park and of his ideas that made the breaking of the Enigma possible, with a concise analysis of the whole spectrum of his mathematical and scientific achievements that won him, among others, the title of 'father of computing'. The story of Colossus, a machine built to break a code far more complex even than Enigma, the cipher machine called Lorenz, used by the top level of German High Command including Adolf Hitler comes next. The team that broke Lorenz is described, showing how a small group of mathematicians, engineers and linguists, who each brought their different skills to the problem, was able to work in collaboration, which was a central theme of this project. Finally the story is brought up to date with the scope of today's 'codebreaking' and the extent to which cryptography is relevant to many aspects of our modern lives. Examples illustrating how most of us use code without even thinking about it, or how cryptography also affords us privacy in our vastly connected world, are presented appropriately here.

Beyond the connections between classicists/linguists and mathematicians/computer scientists, vividly represented in this volume, there is yet another similarity between the two disciplines and that is no other than the joy of breaking codes. One reason we still find it difficult to read codes is because we may have very limited understanding of their intended use, or of the societies that produced them. This is why so much joy attends any new developments. This applies equally to the linguist acquiring a rare glimpse of the ancient world who produced the deciphered text, or to the modern-day cryptanalyst decoding an encrypted message, even if this does not involve stealing the enemy's secrets. We hope this volume's readers will realize, in these pages, an almost equal sense of discovery.

Acknowledgements

The editors are indebted to our lenders at the Ashmolean Museum, the Victoria and Albert Museum and the Government Communications Headquarters. We are also particularly grateful to King's College, Cambridge and the College's senior archivist, Dr Patricia McGuire for guiding us through a complicated process of acquiring permits to publish images and information of the Alan Turing Archive, as well as to Trinity College, Cambridge for allowing us to publish images of the Cambridge codebreaker William Tutte. This volume would not have been produced without the dedication and professionalism of our copy editor and designer Dr Paula Turner, to whom we are all three very grateful.

In particular, Anastasia Christophilopoulou is indebted to the former Keeper of the Antiquities Department, Dr Lucilla Burn for her strong support and encouragement during the early phases of this project, and to the Director of the Fitzwilliam Museum, Tim Knox, for his ongoing support and advise on the production of the book and the building of the exhibition. Anastasia is also indebted to her curatorial colleague Helen Strudwick for reading and commenting on earlier versions of this book as well as to the entire Antiquities team at the Fitzwilliam, Jenny Marchant, Julie Dawson, Charis Millet and Louise Jenkins, all of whom provided much support during the preparation of this volume and exhibition. Our exhibition team, David Evans and Hannah Kershaw, have also offered invaluable advice for matters concerning the book and David Packer and Eleanor Saggers, Fitzwilliam Museum registrars have provided much help in securing image permissions from lenders. Anastasia would also like to thank Professor Andrew Blake, Research Director at the Alan Turing Institute and former Laboratory Director of Microsoft Research Cambridge as well as Sir Tony Hoare, Professor Emeritus, University of Oxford and associated Researcher, Microsoft Research Cambridge, for his encouragement and support, Dr Pippa Steele and Professor Robin Osborne, both Faculty of Classics Cambridge, for assisting her with archival research in preparation for this volume.

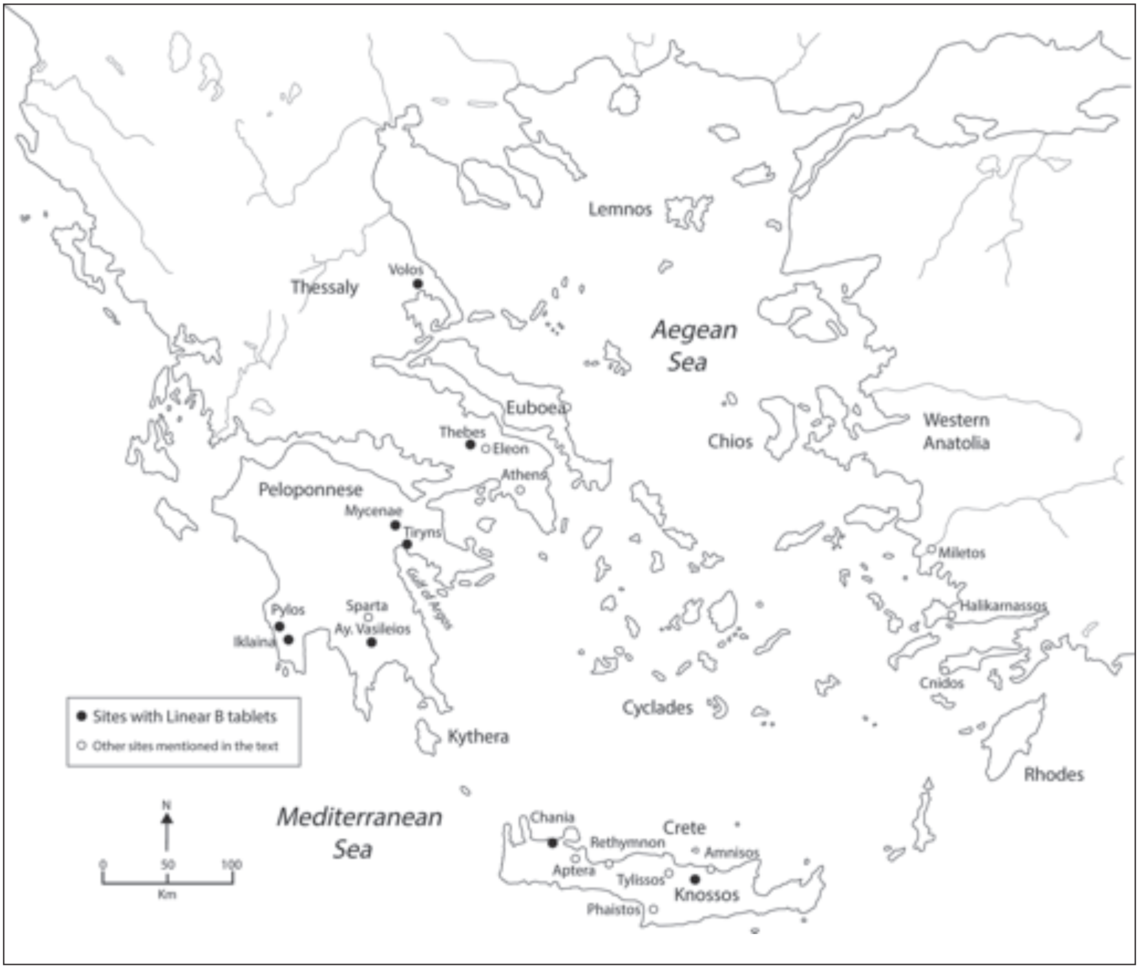
Yannis Galanakis would like to thank the Faculty of Classics for all the support in the making of this exhibition, and Sophie Hawkins, for organizing *Codebreakers* in the Museum of Classical Archaeology. Also

Professor John Bennet, Dr Sally Crawford, Dr Anna Judson, Dr Torsten Meißner, and Dr Katharina Ulmschneider for their assistance in the writing of this catalogue. Special thanks to the staff of the Ashmolean Museum, particularly Dr Anja Ulbrich, Alison Roberts, Amy Taylor, Alice Howard, and to Elizabeth Bray of British Museum Images.

James Grime would like to thank Dr Andrew Shields of Toshiba Research, Cambridge, for his help with Quantum Key Distribution, Dr Jasmina Lazic of Mathworks, Cambridge, for her support of the exhibition, Dr Craig Heath for his wonderful Enigma app and twitter feeds, Claire Butterfield for her amazing Bletchley Park knowledge and Mei Roberts for allowing us to view material left by Captain Jerry Roberts and her continuing championing of the story of Lorenz.

Part 1

The Decipherment of Linear B



Map 1 Sites in the Aegean where Linear B tablets have been found

1

Discovering Writing in Bronze Age Greece

Yannis Galanakis

The decipherment of the Linear B script in 1952 by Michael Ventris, one of the two protagonists of the *Codebreakers and Groundbreakers* project, is considered one of the most astonishing intellectual achievements in the fields of linguistics and archaeology, of comparable fame to the decipherment of the Egyptian hieroglyphs in the nineteenth century. Yet the discovery and naming of the scripts is owed to Sir Arthur Evans (1851–1941), pioneer of the archaeology of prehistoric Crete (3200–1000 BC) who is today mostly remembered for his excavations at Knossos.

Arthur Evans was the eldest child of John Evans and Harriet Ann Dickinson. His father, who made his fortune in the paper manufacturing industry and distinguished himself in archaeology, numismatics and geology, exercised considerable influence on young Arthur. After studying at Harrow, Arthur went up to Oxford, graduating in 1874 with a degree in history. During his university holidays, he would often go travelling across continental Europe and Scandinavia. His eagerness for exploration took him for a month through Bosnia and Herzegovina. He not only investigated the archaeology of the region, and the language and customs of its people, but also entered the political arena. Evans supported the oppressed peasants in their struggle to overthrow their Ottoman Turkish overlords. He wrote about his experience in *Through Bosnia and Herzegovina on Foot*, partly an adventure story and partly an historical, archaeological and political account. This publication established him as an authority on the Balkans, an expertise that secured his first proper job as correspondent for the *Manchester Guardian* in the region (1877–83).

In 1878 Evans married Margaret Freeman and settled in Ragusa (modern Dubrovnik, Croatia). In his role as a correspondent he continued to travel, discovering archaeological sites, and to enjoy the social life of Dalmatia. However, he soon came to dislike the Austrian rule of the region, as much as he disliked the Ottoman Turkish administration. His anti-Austrian reports and activities led to his imprisonment and eventual expulsion from the area in 1882. Waiting for the next professional opportunity to arise, he embarked with his wife on a five-month tour of Greece and neighbouring lands. In 1883 they met the Schliemanns in Athens and visited Mycenae.

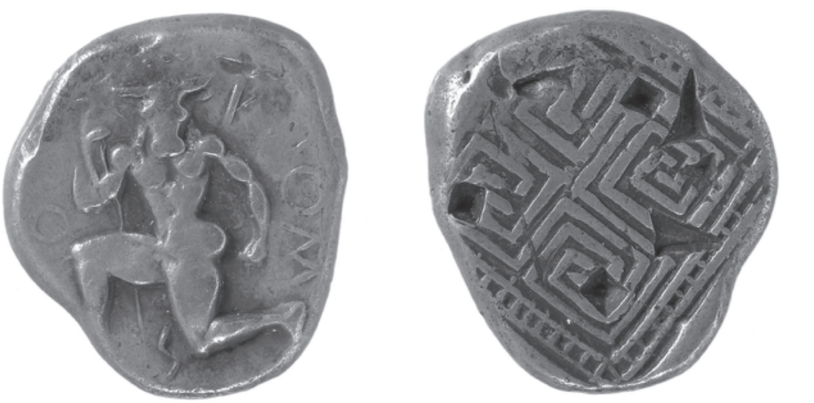


Figure 1
The Minotaur (half-man, half-bull) and the labyrinth on a silver coin from Knossos, about 500 BC (Fitzwilliam Museum, CM.MC.7050. Courtesy of the Fitzwilliam Museum, University of Cambridge)

The discoveries of Heinrich Schliemann in the 1870s, first at Troy in western Turkey and then at Mycenae and other sites on the Greek mainland, astonished the world with the richness, complexity and diversity of finds associated with eras hitherto only known through myths and legends. Schliemann's discoveries seemed to bring the 'heroic times' of Greece back to life. Soon after the scholarly community became preoccupied with explaining the origins of Mycenaean culture. Evans, who had already heard of Schliemann's Trojan discoveries and had seen the 'Treasure of Priam' on display in London, saw in Athens the spectacular finds from the Mycenae shaft graves and had his first hands-on experience with the emerging field of Aegean archaeology.

In 1884 Evans became Keeper of the Ashmolean Museum in Oxford. His work there included adding substantially to the collections and helping to transform the Ashmolean into the museum of art and archaeology of international fame that it is today. With some 215 days of leave a year, he had a lot of time at his disposal for travelling and collecting, often thousands of objects per year. At the time, however, his academic interests, wide-ranging as they were, did not seem to include Aegean archaeology. This change in his interests is first recorded in 1891–2. In February 1892 Evans met in Rome the epigraphist and archaeologist Federico Halbherr, who had been working on Crete for some years. This island was mostly known to Europeans in late nineteenth century through its myths and legends, with the labyrinth of the Minotaur forming its most celebrated story (figure 1). In the words of his half-sister, Joan Evans, 'What [Halbherr] told him of the earlier remains on the island, unexplored and unexplained, fired his imagination and confirmed his interest, though as yet his purpose was hardly formed.'[1] Throughout the rest of the year, Evans started exploring systematically the origins and affinities of Mycenaean culture.

Following the death of his wife in 1893, he dedicated more time and energy to his Aegean pursuits. Schliemann's discoveries at Mycenae had revealed a highly developed prehistoric civilization but found no evidence for literacy. Evans, following the thinking of his time,[2] could not believe that the Bronze Age civilization of Greece was illiterate and began to search for

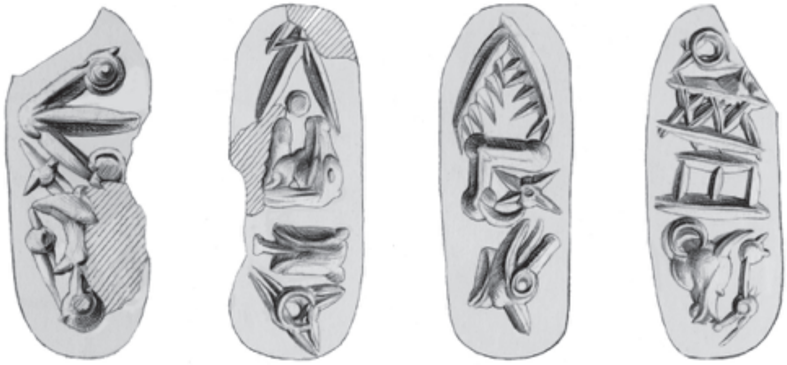


Figure 2
Drawing showing the four engraved sides of the Chester seal (Ashmolean Museum, AN1889.998. Courtesy of the Ashmolean Museum, University of Oxford)

clues of a prehistoric writing system. He visited Athens, where he met John Linton Myres, a young Oxford graduate, who became his lifelong friend. Through discussions with scholars, inspection of the Athens museum collections, and purchases in the art market, Evans became convinced that his theory, on the existence of pre-alphabetic writing, was right.

When he returned to Oxford, he found an unclassed stone which had been brought back by Reverend Greville Chester from Greece. Chester had bought the seal in the art market in Athens in the 1880s and knew little of its significance (figure 2). In 1889 Chester gave this tiny, four-sided, stone along with a few other seals and antiquities to the Ashmolean – the 'rediscovery' of this seal, along with Evans's purchases in Athens, added further weight to his hypothesis.

In a lecture in London on 27 November 1893 Evans announced that a system of picture-writing once existed in the Greek lands, as a number of engraved gems seemed to suggest. The best place to look for more evidence to support his idea further was the island of Crete, where most of these gems appeared to originate according to the specialists of the time, most prominently Arthur Milchhöfer, who also suggested that the origins of the Mycenaean culture should be sought in Crete. Myres, encouraged by Evans, visited Crete in 1893, where he investigated the trenches dug by Minos Kalokairinos at Knossos. Kalokairinos, a local businessman and antiquarian, had excavated part of the palace in 1878–9, finding giant *pitharia* (storage jars). Myres saw large masonry blocks with curious incised signs and confirmed the importance of the site, as many other scholars had done before him, including Schliemann and Halbherr. In addition, Myres also saw more engraved gems on the island convincing Evans that Crete was an island worth exploring further.[3]

Through his travels in Crete (1894–9), Evans developed an expertise on the island's history, material culture and local politics. He also purchased many seal stones; his Ashmolean collection of more than 550 gems is today the largest outside of Greece. Everywhere he went, he sought to buy *galopetres* (milk stones), as these ancient gems were locally known, worn by village women to ensure a plentiful milk supply for their babies. Midway through his first campaign on the island, on 25 April 1894, Evans could not contain his excitement when he announced a 'Mycenaean system of writing in Crete and the Peloponnese' in *The Athenaeum*:

> the evidence supplied by these Cretan finds shows that long before the alphabet was first introduced into Greece, the Aegean islanders . . . had developed an independent system of writing. Of this writing there were two phases, one pictographic . . . the other linear. This latter system was certainly a syllabary, in part at least identical with that of Cyprus, perhaps indeed its direct progenitor.[4]

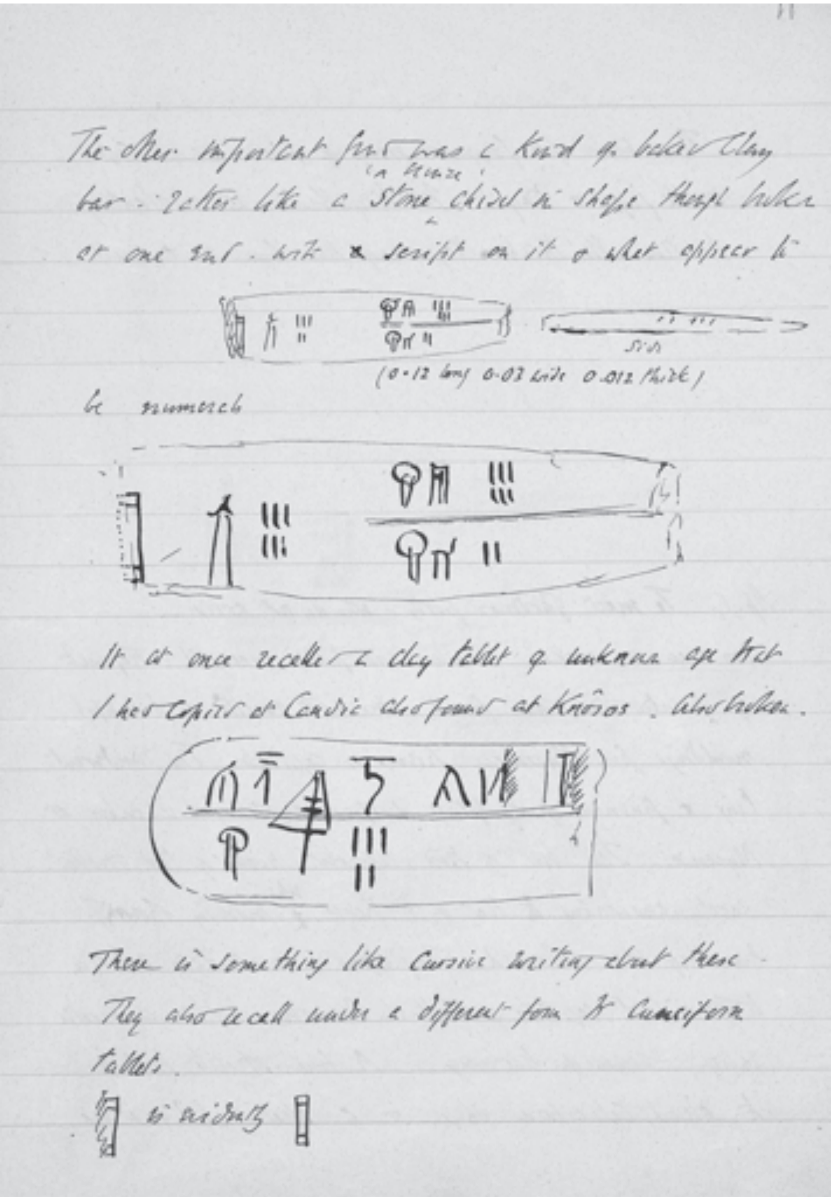
To the world's astonishment, Evans had identified not one, but two systems of pre-alphabetic writing: the first, found on seal stones, he called 'Pictographic' or 'Hieroglyphic' (though there is no connection to Egyptian hieroglyphs), and the second system 'Linear'. Either in 1895 or 1896 he had also come across a burnt clay fragment, said to be from Knossos and most likely from Kalokairinos's excavations, that presented some incised Linear signs which seemed to belong to 'an advanced system of writing'.[5] In his study on *Cretan Pictographs and Pre-Phoenician Script*, Evans put forward his theory on the relationship between these systems, supposing a unidirectional process of script development from pictographic to more linear forms. His achievement was heralded by his contemporaries as 'a triumph of learning and skill . . . likely to bear important fruit for the archaeology of the eastern basin of the Mediterranean'.[6]

Four days after his arrival to Crete in 1894, Evans paid his first visit to the Kephala hill at Knossos and saw the ruins unearthed during Kalokairinos's excavations. Subsequent visits confirmed the importance of this hill. He was determined to excavate, although he had first to purchase the land and wait until the political situation on the island was resolved. Finally, in 1900 he completed the purchase and was at last able to fulfil his dream: to excavate Knossos and uncover examples of writing in context. Until then Evans relied exclusively on his stylistic analysis for dating the inscriptions he had identified (figure 3).

Just a week into the first archaeological season at Knossos, Evans and his team, led by Duncan Mackenzie, made an important discovery: 'a kind of baked clay bar, rather like a stone or bronze chisel in shape though broken at one end, with a script on it and what appeared to be numerals'. On 5 April 1900 an entire hoard of clay documents came to light, many of them in perfect condition (figures 4 and 5 overleaf).

> The marvel is that any of these clay tablets should have resisted the natural dampness of the soil, and in many cases their survival was due to the extra baking they received through the conflagration of the building. In this way, fire – so fatal elsewhere in historical buildings! – has acted as a preservative of these earlier records.[7]

In 1902 Evans's friend and inspiration Federico Halbherr made a discovery at Ayia Triada in south Crete of numerous tablets inscribed in



11

The other important find was a kind of baked clay bar – rather like a stone chisel in shape though broken at one end – with a script on it & what appear to be numerals

'a bronze'

(0·12 long 0·03 wide 0.012 thick)

It at once recalled the clay tablet of unknown age that I have copied at Candia also found at Knosos. Also broken.

There is something like cursive writing about these. They also recall under a different form the Cuneiform tablets.

is evidently

Figure 3
Page 11 of Arthur Evans's excavation notebook illustrating a Linear B tablet that he unearthed on 30 March 1900, shortly after the beginning of his work at Knossos. This discovery made him recall a similar document that he had seen at Herakleion in the 1890s 'of unknown age . . . also found at Knossos'
(Courtesy of the Ashmolean Museum, University of Oxford)

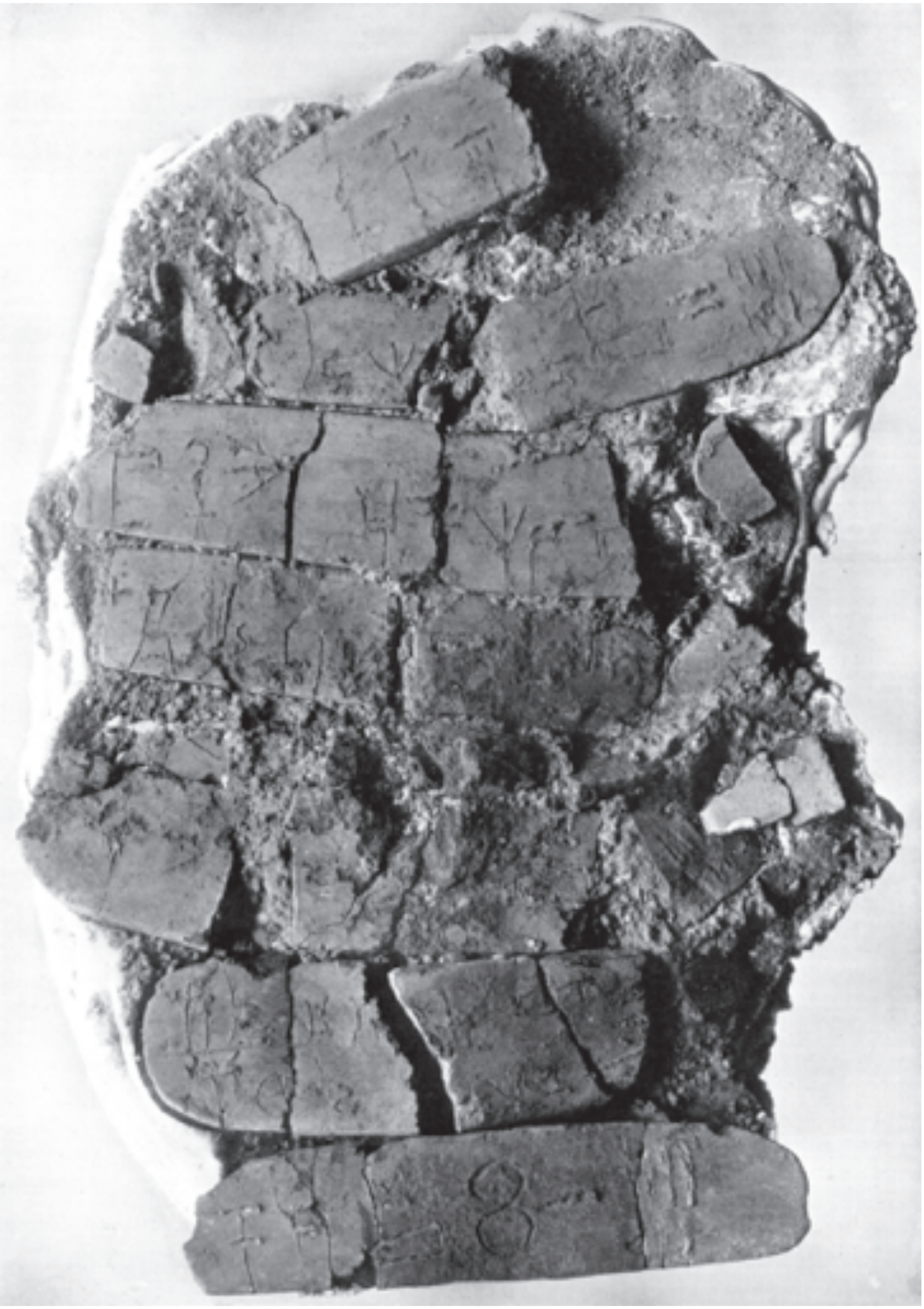
the 'linear script'. They were very similar to the documents from Knossos which were predominantly inscribed in the 'advanced linear script', but somewhat earlier in date and showing some differences. This led to the identification of a 'Linear A' and a 'Linear B' class of writing. By 1903 Evans was convinced that Cretan Hieroglyphic was the earliest script on the island, followed in later times by Linear A and subsequently Linear B (on Cretan Hieroglyphic and Linear A see chapter 4). In total Evans discovered some 3,400 Linear B documents during his excavation at Knossos (almost 65 per cent of all known examples to date), including

Figure 4
Evans with finds from his Knossos excavations in 1900
(Courtesy of the Ashmolean Museum, University of Oxford)

Figure 5 opposite
Knossos Linear B tablets as removed from the ground
(From Evans 1935, 670, fig. 655)

some in Hieroglyphic and a few in Linear A. This discovery laid the foundations for the systematic study of these three pre-alphabetic scripts.

Although Evans never deciphered Linear B, he was right in a number of observations: for example, he identified the left-to-right direction of writing, he recognized correctly the use of a decimal system of numeration and was the first to point out the existence of metric signs and ideograms – signs standing for people, animals, objects and commodities. Evans also identified the signs for 'man' and 'woman'. On the basis of long lists of what looked like personal names followed by these signs, he assumed the existence of feminine and masculine endings. He also identified word dividers, and the nature and number of the syllabic signs (around



ninety). Indeed, Evans knew that he was dealing with a syllabary and not an alphabet: Linear B used a set of signs some of which represented syllables (a consonant and a vowel) and others just vowels (see chapter 2). Moreover, he suspected that the texts were largely bureaucratic in nature.

Two more observations were to pave the way for the decipherment of Linear B many years later: in 1927, in a volume in honour of Evans, Sir Arthur Cowley (1861–1931), Oxford's Bodleian Librarian and leading Semitic scholar, made some very important observations in his three-page article, 'A Note on Minoan Writing'.[8] Cowley observed that the later, though related, Cypriot Syllabary had six signs identical to Linear B, while many other signs bore close resemblance.[9] Could these values have been the same in Linear B? From the material available to him (which was not much!), Cowley speculated that the language behind Linear B was probably inflected: the end of a word was important for specifying gender and number. But he did not stop there: he also suggested that two groups of signs listed together with the 'woman' sign in a clear context of numerical calculations should be identified as 'boy(s)' and 'girl(s)' – an ingenious postulation, which with minor modifications was proved right by the decipherment of Linear B. Evans accepted both of Cowley's identifications, and in his final volume on the Knossos excavations, *The Palace of Minos* volume IV in 1935, concluded that the Linear B documents offered 'good evidence of declension'.[10]

Despite these advances, however, three main issues prevented attempts for deciphering Linear B: first and foremost, the lack of a complete publication that would bring together, in photographs and drawings, all documents from Knossos. Evans had indeed planned such a publication, entitled *Scripta Minoa*: *The written documents of Minoan Crete with special reference to the archives of Knossos*. This publication was meant to follow the publication in 1909 of the Cretan Hieroglyphic documents from Knossos. However, work on the voluminous *Palace of Minos* – a compendium of his excavations and of the Bronze Age art and archaeology of Crete – and his own ambition to decipher the script delayed *Scripta Minoa* which only appeared posthumously, edited by his old friend Myres.

The second issue was Evans's evolutionary approach to the subject of writing. A convinced Darwinist, he was preoccupied with detecting the evolutionary origins of each sign back to 'a hypothetical seed-bed of very primitive picture-writing'.[11] In this matter he followed mostly the ideas of Edward Tylor, pioneering anthropologist and a close friend of his father. Tylor regarded writing as a measure of human progress and saw its origins in gesture language turned picture writing and later, through a process of mixed pictographic and conventional signs into more advance systems, culminating eventually in the alphabet.[12] Evans's identifications and 'readings' of signs stemming from this approach were, simply put, impossible to prove right or wrong without prior knowledge of the history of the letter forms under study which in the case of the Aegean scripts was and still is lacking. For example, Evans thought that the sign now deciphered by Ventris as *a* represented a double axe (𐀀) and had a religious connotation in the inscriptions where it occurred – a major barrier in how the script and its signs should be understood and in the script's decipherment.

A third obstacle hampering attempts to better understand Linear B was Evans's broader views on the socio-political organization of the Aegean Bronze Age. When he started his excavations at Knossos, he thought without hesitation that he was uncovering another Mycenaean palace, as Schliemann had done before him. Therefore he assumed that the scripts he identified there were also 'Mycenaean'. However, it became clear to him through his excavations at Knossos, and especially from 1902 onwards, that the material culture he and his team were discovering was earlier and distinct from that of mainland Greece. This observation made him start using the term 'Minoan' to describe his discoveries, the Cretan culture and its pre-alphabetic scripts. Since Linear B was to be understood as a development of Linear A, they both represented for Evans the Cretan language – an unknown language, but one that surely could not have been Greek.

Searching for the origins of 'Mycenaean culture' since the early 1890s, Evans had now been convinced that Crete was the source of inspiration he was looking for. He actually suggested that there was a 'universal occupation of mainland Greece by men of Minoan stock'.[13] It was only after 1400 BC, when Knossos was destroyed, by an earthquake according to Evans, and its Linear B documents were baked, that Mycenaean polities started to rise independently of Crete. Therefore, the few pots bearing Linear B inscriptions on the mainland were for Evans nothing else but further evidence of his colonization theory.

His conviction that the language of Linear B was unrelated to Greek was almost universally accepted and would perplex scholars down to 1952 and just a few months prior to the decipherment. However, his 'Minoan domination' idea had already started to be questioned, first and foremost by Alan Wace, Director of the British School at Athens and later Laurence Professor of Classical Archaeology in Cambridge, and by Carl Blegen of the University of Cincinnati, a friend of Wace and an outstanding Aegean archaeologist himself. Through their excavations, Wace and Blegen came to the conclusion that mainland culture grew independently of the island's influence.

Although Evans seemed to temporarily win the debate, the question of Mainland–Cretan relations was rekindled following the astonishing discovery by Blegen and his Greek collaborator, Konstantinos Kourouniotis, in 1939 of more Linear B tablets – this time, however, not on Crete, but for the first time in large numbers and in the same form as in Crete, at Ano Englianos, Bronze Age Pylos, the so-called 'Palace of Nestor' in the south-western Peloponnese. Blegen and his team found the tablets on the first day of excavation, just a couple of hours after they had broken ground. They soon realized, however, that unlike Evans's early dating for the Knossian documents, the Pylos tablets dated to around 1200 BC. Both sides of the debate were perplexed by this discovery: Evans saw in them the final confirmation of his theories, suggesting to Blegen that the fact that the date may not square chronologically with his findings from Knossos should not surprise him; while Wace prophetically noted to Blegen in 1940, 'We all hope your tablets will turn out to be in Greek and not in the Minoan language.'[14]

Despite his controversial ideas, shortcomings and fixations, Evans will always be credited as having identified the three pre-alphabetic scripts in the Aegean and making notable observations that paved the way for the breaking of the Linear B code. In 1936, at the age of eighty-five, he arranged an important exhibition in Burlington House in London, part of the 'British Archaeological Discoveries in Greece and Crete' exhibition that celebrated the fiftieth anniversary of the founding of the British School at Athens. Evans was responsible for the 'Minoan Room', which illustrated his recent discoveries at Knossos. Lectures were held in conjunction with the exhibition. On one of these occasions, a group of boys from Stowe School came to visit. Among the students there was a fourteen-year-old boy, Michael Ventris, who followed Evans's tour and became fascinated by the specimens of the Linear script that were on display near the entrance to the exhibition, in 'Desk Case L'.[15] According to Patrick Hunter, Ventris's classics teacher at school, the young boy asked Evans, 'Did you say the tablets haven't been deciphered, Sir?'[16] Thus began a life-long fascination of Ventris with the 'Minoan problem', as research on the language of the Linear B documents came to be known.

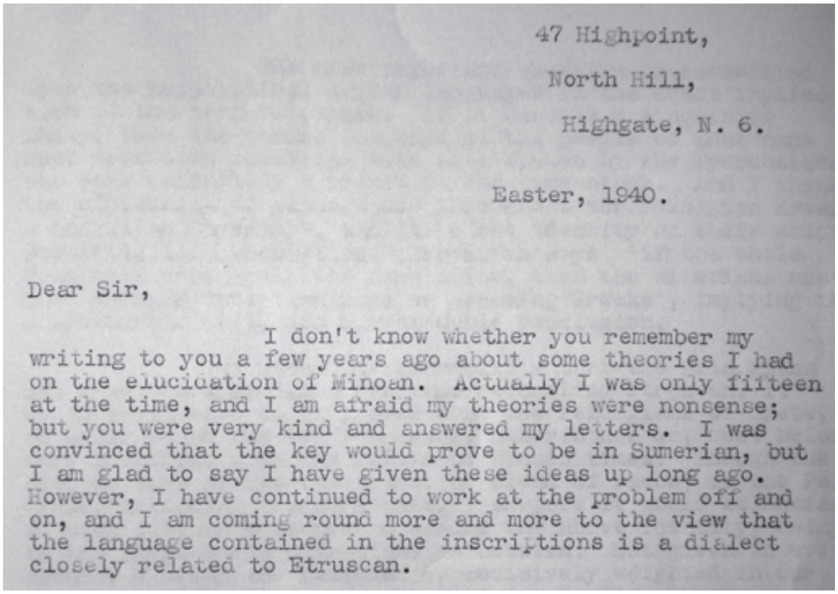
Ventris got in touch with Evans in 1938 and again at Easter 1940 (figure 6). His determination to work on the problem of Linear B is noteworthy:

> I am convinced that now [more] than ever before is the time for a decisive and concerted effort to liquidate the problem.[17]

Evans's support paid dividends with Ventris, by now eighteen years old, publishing his Etruscan theories in the highly respected *American Journal of Archaeology*.

When Evans died in 1941, little was ready for *Scripta Minoa* except photographs and technical plans for printing. The unenviable task of publishing the Linear B documents from Knossos fell on John Myres, his travel companion in his early journeys to Athens and Crete. Myres was a man of many talents: a classicist, archaeologist, historian, geographer, father of Cypriot archaeology and a pioneer in applying anthropology to the study of ancient societies (figure 7). Recognizing the limits of his knowledge, Myres actively enlisted help, especially for checking the transcriptions of the documents, from the numerous scholars working on Linear B at the time.

Although scholarly work continued in the 1940s, the Second World War prevented access to the original material and hampered communication. Despite the major delay Myres continued to work on the publication of *Scripta Minoa*, enlisting help from every direction. Soon after Evans's death, he even contacted Michael Ventris, informally mentoring him in



47 Highpoint,
North Hill,
Highgate, N. 6.

Easter, 1940.

Dear Sir,

I don't know whether you remember my writing to you a few years ago about some theories I had on the elucidation of Minoan. Actually I was only fifteen at the time, and I am afraid my theories were nonsense; but you were very kind and answered my letters. I was convinced that the key would prove to be in Sumerian, but I am glad to say I have given these ideas up long ago. However, I have continued to work at the problem off and on, and I am coming round more and more to the view that the language contained in the inscriptions is a dialect closely related to Etruscan.

Figure 6
Extract from a letter sent by Michael Ventris to Arthur Evans, Easter 1940; note the remark about Ventris's age (Courtesy of the Ashmolean Museum, University of Oxford)

his Linear B studies (figure 8 overleaf). As the person responsible for the Knossian documents, Myres was contacted frequently by numerous scholars asking permission to access and study this material. It has to be said that, with a few exceptions, co-operation had not been remarkable on Linear B studies, so when Alice Kober (1906–50), a talented linguist and an academic in New York, asked Myres if she could see the material he had in his possession, she was surprised to receive Myres's open-handed

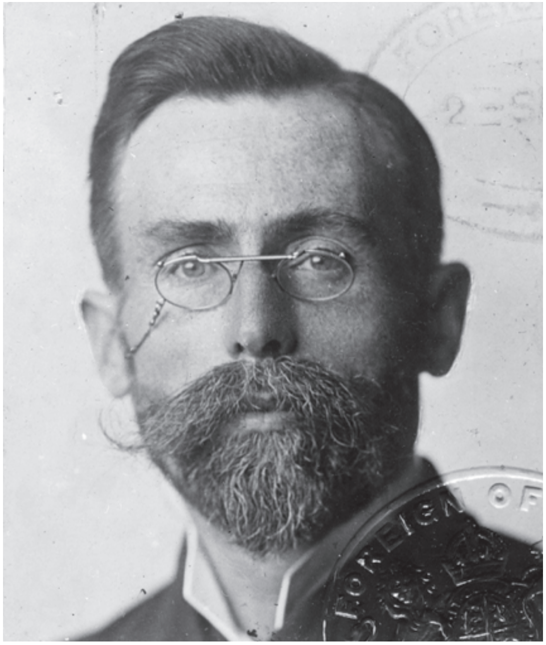
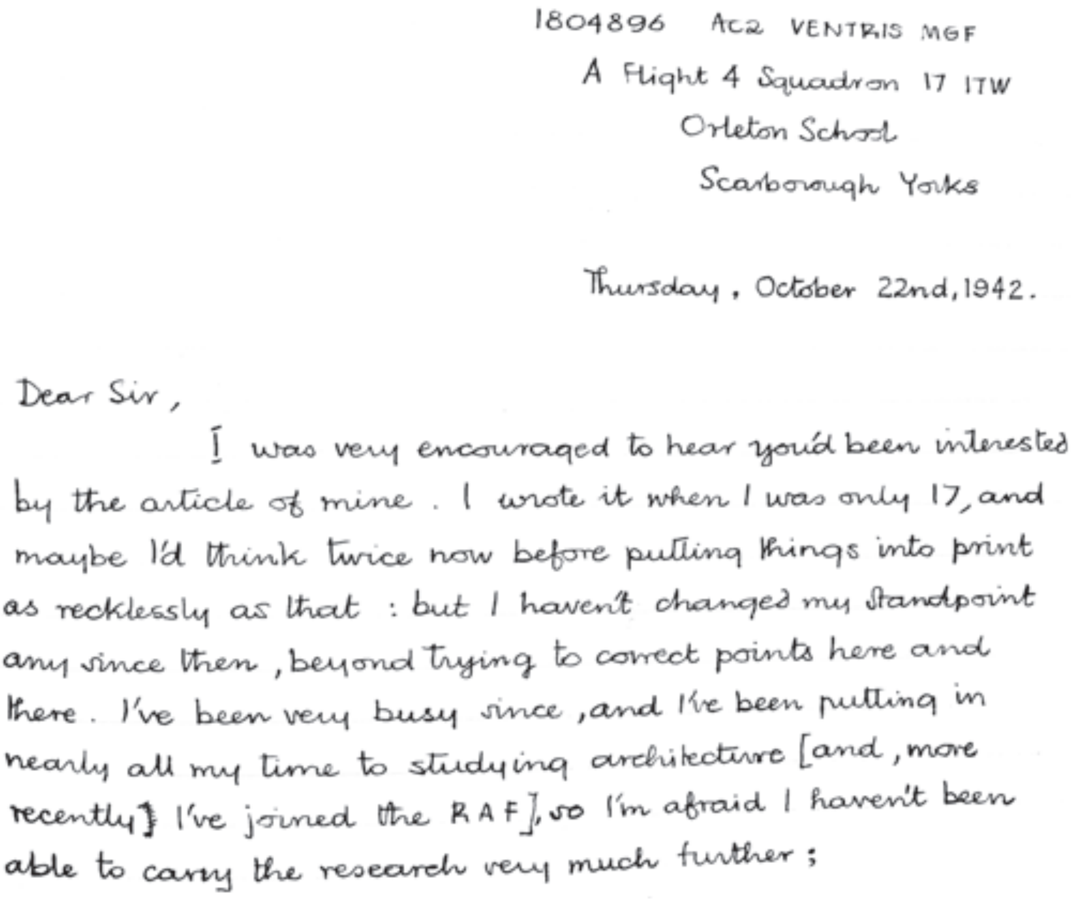


Figure 7
John Linton Myres, passport photograph dated 1921
(Myres Archive, reproduced courtesy of the Institute of Archaeology, University of Oxford)



1804896 AC2 VENTRIS MGF
A Flight 4 Squadron 17 ITW
Orleton School
Scarborough Yorks

Thursday, October 22nd, 1942.

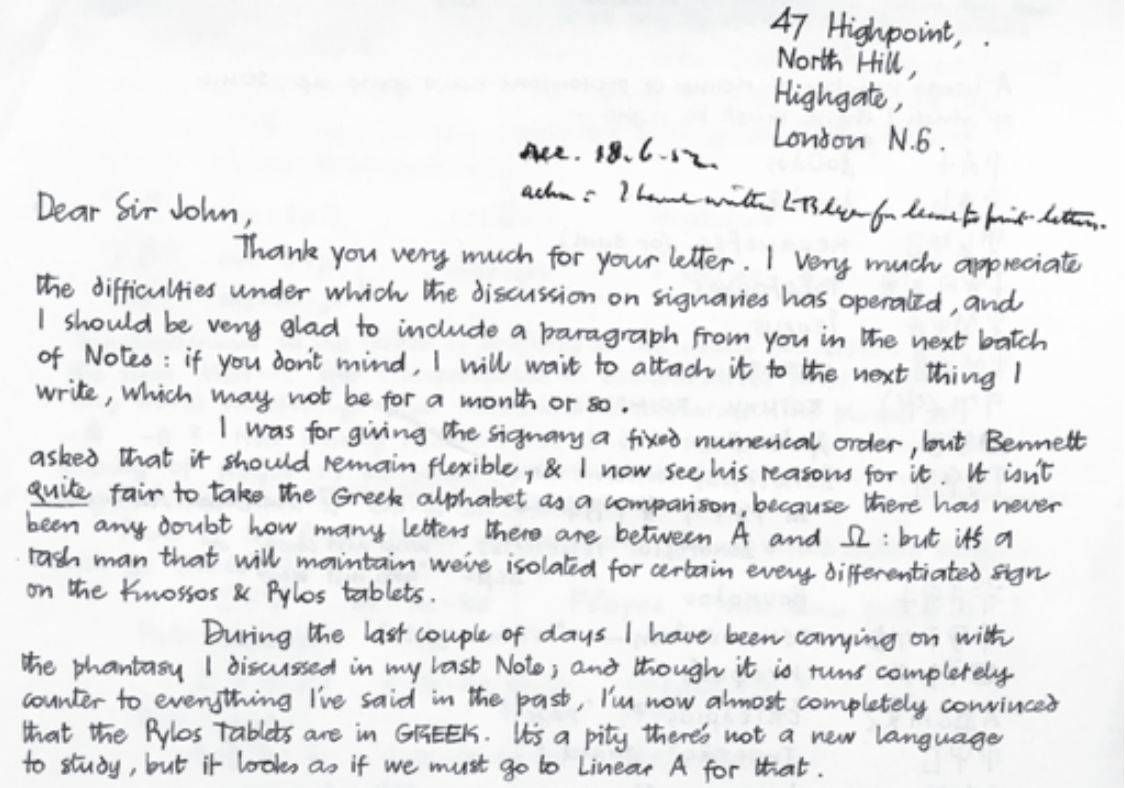
Dear Sir,

I was very encouraged to hear you'd been interested by the article of mine. I wrote it when I was only 17, and maybe I'd think twice now before putting things into print as recklessly as that: but I haven't changed my standpoint any since then, beyond trying to correct points here and there. I've been very busy since, and I've been putting in nearly all my time to studying architecture [and, more recently] I've joined the RAF], so I'm afraid I haven't been able to carry the research very much further;

Figure 8
An early letter of Michael Ventris to John Myres, 22 October 1942 (Courtesy of the Ashmolean Museum, University of Oxford)

generosity. She not only gained access but became his chief collaborator in the publication of *Scripta Minoa* from 1947 to 1950, the year of her untimely death (for Kober's important contribution to Linear B see chapter 2).

More support came to Myres from Emmett Bennett (1918–2011), especially after the war and following Kober's death. Bennett was a student of Blegen and was entrusted by him to research 'The Minoan Linear Script from Pylos' for his doctoral dissertation (completed in 1947 without access to the original material). Bennett produced the first accurate list of Linear B signs (signary) that allowed valid statistical analyses to be performed on their pattern of occurrence in the Knossian and Pylian documents. The spirit of mutual co-operation, team effort and information sharing was being established, a spirit that has played a crucial role in speeding up the decipherment and a characteristic of Linear B studies to this day. The publication of the Pylos tablets in 1951 by Bennett and of the Knossian documents finally in spring 1952 by Myres meant that a much larger corpus of inscriptions was now available for study offering an opportunity for a breakthrough (see chapter 2).



47 Highpoint,
North Hill,
Highgate,
London N.6.

Acc. 18.6.52.
ackn: I have written to Blegen for leave to print letter.

Dear Sir John,

Thank you very much for your letter. I very much appreciate the difficulties under which the discussion on signaries has operated, and I should be very glad to include a paragraph from you in the next batch of Notes: if you don't mind, I will wait to attach it to the next thing I write, which may not be for a month or so.

I was for giving the signary a fixed numerical order, but Bennett asked that it should remain flexible, & I now see his reasons for it. It isn't quite fair to take the Greek alphabet as a comparison, because there has never been any doubt how many letters there are between A and Ω: but it's a rash man that will maintain we've isolated for certain every differentiated sign on the Knossos & Pylos tablets.

During the last couple of days I have been carrying on with the phantasy I discussed in my last Note; and though it is runs completely counter to everything I've said in the past, I'm now almost completely convinced that the Pylos Tablets are in GREEK. It's a pity there's not a new language to study, but it looks as if we must go to Linear A for that.

Figure 9
Michael Ventris writing his frivolous digression to John Myres, received on 18 June 1952
(Courtesy of the Ashmolean Museum, University of Oxford)

Although Ventris seemed to have temporarily given up Linear B at the end of the 1940s for architecture, his main employment, he came back more determined than ever. From 1951 Ventris began to send to anyone interested in Linear B his *Work Notes* of his research on the Minoan language. Just a few weeks before his announcement on the BBC's Third Programme (now Radio 3) on 1 July 1952 (at prime time, 7.20 p.m.), and shortly after the publication of *Scripta Minoa,* he wrote to Myres to say that 'I'm now almost completely convinced that the Pylos tablets are in GREEK'[18] (figure 9 and p. 23 below).

Myres, who was very sceptical at the beginning of this development, was eventually convinced, with some help from John Chadwick (1920–1998), a young lecturer in classical linguistics at Cambridge, who was to become a co-decipherer. Chadwick wrote on 9 July 1952 to Myres, 'I think we must accept the fact that a new chapter in Greek history, philology and epigraphy is about to be written.'[19] Myres introduced Chadwick to Ventris and the two men made further progress on the language, structure and contents of Linear B. Ventris's ground-breaking decipherment created indeed a new field of study – Mycenology – which gave access to new data in terms of language and archaeology (see chapters 2 and 3).

In 1952 more tablets were discovered, at Mycenae by Wace and at Pylos by Blegen. The old controversy with Evans was rekindled in the light of

Ventris's breaking of the Linear B code. In the decipherer's own words,

> the last palace of Knossos has all the appearance of being part of the native island culture; but if my suggestion is right, the Greeks must in fact have arrived in Crete at its building and not merely being its destroyers. If this is so, there is a case of calling the tablets which Myres and Bennett published Mycenaean and not Minoan in a strict sense'.[20]

Although Evans' 'Minoan domination' idea was waning, explaining the appearance of Linear B, first on Crete and subsequently in the rest of the Aegean, remains an issue of discussion among scholars.

Since the 1950s a lot more sites have yielded documents inscribed in Linear B, including more material at Pylos and Mycenae (in the 1950s and 1960s), Thebes in Boeotia (1964–), Tiryns in the Argolid (1966–), Chania in Crete (1989–), Volos in Thessaly (2009, but excavated in 1956–61) and Iklaina in Messenia (2010–) (see map on p. xvi). The single most important discovery, made in the last decade, has been the unearthing of more than 150 Linear B documents, and counting, at Ayios Vasileios in Laconia, a site that appears to be a major regional administrative centre. Despite significant advances in the field and the additional refinement in recent years of improving our understanding of the existing texts, the discovery of new documents will continue to surprise us and enrich our knowledge on the people of Linear B and their world.

The presence of high-quality visual media and searchable online databases has recently helped increase further the visibility of Linear B not only to a scholarly audience but to one that is in general interested in learning more about early writing and the societies that made use of this tool (see chapter 5). As Ventris had foretold, 'There is now a better chance of reading these earliest European inscriptions than ever before, but there is evidently a great deal *more work to do* before we are all agreed on the solution of the problem.'[21] Although Ventris was referring to his decipherment, his words resonate well with our continuing efforts to better understand the language, documents, economy and wider interests of Linear B administration.

Any decipherment offers a window to the cultural codes of the era that produced and made use of writing. How to read these codes, however, remains a matter of research and debate. The discovery of writing in the Aegean and the subsequent decipherment of Linear B are only the beginning. What surprises lie ahead?

2

The Decipherment: People, Process, Challenges

Anna P. Judson

Linear B before the decipherment: facts and theories

When Linear B tablets were first discovered – at the palace of Knossos on Crete, excavated initially by Minos Kalokairinos in 1878 and then by Sir Arthur Evans from 1900 onwards – archaeologists and classicists were confronted with a double mystery: inscriptions written in a script no one knew how to read, recording an unknown language (see chapter 1). Previous decipherments of unknown scripts had generally relied on identifying the language they recorded and/or the existence of bilingual inscriptions giving the same text in two languages: the decipherment of Egyptian hieroglyphs, for example, had famously made use of the Rosetta Stone, a text written in hieroglyphs, demotic Egyptian and Greek.[1] Similarly, the Cypriot Syllabary, used on Cyprus during the first millennium BC, had been deciphered via an inscription written in both Cypriot and the ancient Semitic language Phoenician, and was consequently shown to be recording the Greek language (see chapter 4).

Without any bilingual texts, and without knowing what language the tablets were written in, attempting a decipherment of Linear B would be much more difficult, but some basic facts could be established even without being able to read the script. First, its signs could be divided into two types: phonetic signs, standing for sounds and used to spell out words; and signs which stood for items or commodities. It was clear that the latter, known as 'ideograms' (i.e. signs standing for concepts rather than sounds or words), were used when counting the objects they stood for, since the numerals were also identifiable (the numbers one to nine were represented by vertical strokes, and tens by horizontal strokes), and some of these ideograms were also clearly pictorial in origin. Thus, 𐂃 𐄈 could be 'read' as 'two horses', 𐂀 𐄑 as 'twenty men', and 𐂁 𐄐𐄋 as 'fifteen women'. Although this gave no information about the language concerned, nonetheless it enabled the basic subject matter of many of the tablets to be understood, and showed that their function was administrative: the palace had used these tablets to record a wide range of goods, livestock and personnel. Even the likely meanings of a few words could be deduced: the terms 𐀵𐀰 and 𐀵𐀭, which frequently appeared at the ends of lists alongside the sum of all the numerical entries, were clearly two different forms of the word for 'total'; a number of tablets listed women followed by two further entries, 𐀒𐀺 and 𐀒𐀷, which were assumed to mean 'boys' and 'girls' (although it was uncertain which was which).

Second, the number of different phonetic signs, around ninety, enabled the script's structure to be deduced. An alphabetic script, in which each sign stands for a single sound, would have far fewer signs (the Roman alphabet used for English has twenty-six signs, the classical and modern Greek alphabet twenty-four); on the other hand a system like the Chinese script, in which signs may stand for whole words as well as individual syllables, would have thousands of signs. Linear B therefore had to be a syllabary, with each sign standing for a syllable, that is, either a vowel (e.g. *a*, *e*) or a combination of consonants and vowels such as *pa* or *te*. Further evidence that this inference was correct was provided by the Cypriot Syllabary mentioned above, a syllabic script containing fifty-five different signs, which was used during a later period to write Greek on Cyprus: some of the signs of this script appeared similar enough to those of Linear B to show that the scripts were related. In principle this could have provided a way into deciphering the Cretan scripts, since the values of the Cypriot signs were already known; however, it was difficult to find more than a handful of signs that might correspond closely enough to make reading the Cretan signs with the Cypriot values unproblematic. Linear B 𐀙 and Cypriot 𐠚 *na*, for instance, looked very similar, making it plausible that they could have the same value; but many more Cypriot signs simply had no clear Linear B correspondences at all. A further complication was introduced by Evans, who, based on the existence of the ideograms, suggested that some of the signs occurring in word sequences also had a pictorial origin: he thought the sign 𐀃, for instance, looked like a 'throne and sceptre', and was therefore a 'determinative' sign acting as an indicator that the words with which it appeared referred to royalty (see chapter 1).

Without knowing the language the texts were written in, this was very far from being enough information to produce a decipherment. Of course, there was no shortage of suggestions as to what the language of the Linear B tablets might be: theories ranged from an Anatolian language, related to those spoken in the area that is now Turkey, to Etruscan, a pre-Roman language of Italy. The one language that was generally ruled out as a possibility was Greek: the 'Minoan' Cretan culture Evans had discovered seemed entirely unlike anything known from classical Greece. Evans himself was convinced – and he convinced many others – that the 'Minoan' language of the tablets could not be Greek.

Progress was initially also hampered by a lack of wider access to the inscriptions. Texts of a small number of Linear B tablets were made available in Evans's publication of the Knossos excavations, *The Palace of Minos*, in 1935,[2] but at the time of his death in 1941 the vast majority of the tablets were still unpublished; they finally appeared in 1952 in *Scripta Minoa* volume II, prepared by the Oxford historian and archaeologist Sir John Myres with considerable help from other scholars, in particular the American classicist Alice E. Kober (see below).[3] In the meantime, more

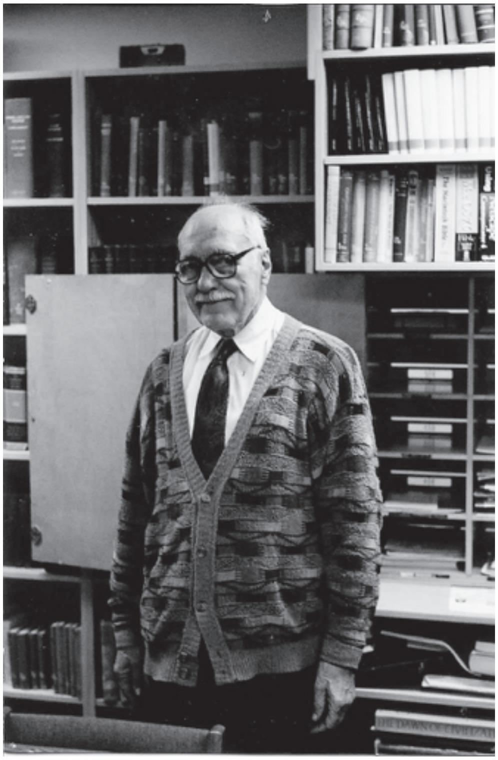


Figure 1
Emmett L. Bennett Junior
(Steven Karanikolas/ Program in Aegean Scripts and Prehistory; reproduced courtesy of Professor T. G. Palaima)

Linear B tablets had been found at Pylos on the Greek mainland, beginning in 1939; but work on these texts was delayed by the Second World War, and they were only fully published in 1951. Thus, the amount of material that was publicly available before the early 1950s was very limited. This did not, however, prevent the publication of several claimed 'decipherments' of the tablets, interpreting them as being in various languages including Greek, Hittite and even Basque, none of which was founded on a rigorous enough methodology to gain widespread acceptance.[4]

Most of the crucial work leading to the eventual successful decipherment of Linear B took place in a relatively short period in the late 1940s and early 1950s, and this chapter will focus on the four people who made the most important contributions to the decipherment during this period: two American classicists, Emmett L. Bennett Junior and Alice E. Kober; one British classicist, John Chadwick; and the British architect who actually achieved the decipherment, Michael Ventris.

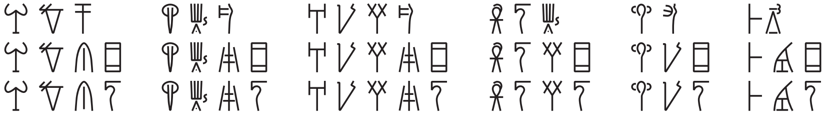
Decipherment in progress: Bennett, Kober, Ventris and Chadwick

Emmett L. Bennett Junior (1918–2011, figure 1)[5] was a postgraduate student working on the Pylos Linear B tablets with Carl Blegen, the excavator of Pylos, at the University of Cincinnati during the 1940s.

After spending the Second World War working as a cryptographer breaking Japanese codes, he returned to Cincinnati to write his PhD thesis. Completed in 1947, this included the first systematic classification of the Linear B signs, establishing the definitive list of signs and their variant forms (which he published in 1951 along with the texts of the Pylos tablets). Just as in English the same letter can look different in different handwriting or fonts (compare ‘a’ and ‘*a*’), so too in Linear B the form of a single sign can vary; in other cases, forms that appeared superficially similar might in fact be separate signs. Consider, for instance, the following two pairs of Linear B signs: 𐀅 and 𐀲; ┬ and ╤. The first pair differs only in whether the horizontal stroke crosses the vertical, the second only in the number of horizontal strokes near the top of the signs. Only a close analysis of all the occurrences of these four forms can show that ┬ and ╤ are in fact variant forms of a single sign – they occur in the same position in what are clearly instances of the same word – while 𐀅 and 𐀲 are different signs. Through his analysis, Bennett also demonstrated that Evans’s ‘determinative’ theory was wrong: signs such as ⎣ were phonetic signs, just like the rest of the syllabary. By establishing the Linear B sign list in this way, Bennett enabled accurate analyses of the script and the occurrences of each sign to be carried out for the first time, laying the foundation for the later decipherment.

After graduating with a PhD from Columbia University, Alice E. Kober (1906–50, figure 2)[6] became an assistant professor of classics at Brooklyn College in New York, but devoted what little spare time she had from her full-time teaching position to tackling Linear B.

As well as being instrumental in the eventual publication of the Knossos Linear B tablets in the second volume of *Scripta Minoa*, Kober undertook a painstaking analysis of the patterns of occurrences of different signs in the available Linear B texts, producing two breakthroughs which would be key to the script’s later decipherment. In a series of articles published in the late 1940s,[7] she demonstrated that, whatever the language of the Linear B tablets was, it must be an inflected one: that is, the endings of its words changed to reflect their grammatical function (as in, for example, English plurals: *sign* vs. *signs*). Kober identified various examples of inflection, in which instances of what seemed to be the same word appeared with different endings in different contexts, for example:



In each column a single word appears in three different forms; two of these forms consistently end with the same signs (𐀍 and 𐀊) regardless of what signs precede the ending. Kober therefore suggested that these signs represented case endings, distinguishing different grammatical functions of nouns. She also showed that the language of the Linear B tablets distinguished words of different genders, by demonstrating that of

Figure 2
Alice E. Kober
(Brooklyn Public
Library, Brooklyn
Collection)

the two different forms of the word identified as 'total', 𐀵𐀰 and 𐀵𐀭, the first appeared alongside 'man' ideograms and the second with 'woman' ideograms, but never vice versa: the different final signs in this instance, at least, therefore represented word endings signifying masculine and feminine gender.

Crucially, Kober then took her identification of patterns of inflection a step further to show how this information could also be used to establish a relationship between different signs' sound values. To take a modern example, the Italian word 'good' is *buon**o*** (masculine), *buon**a*** (feminine): written in syllabic form these would be written as *bu-o-**no***, *bu-o-**na***. The final syllables would be written with different syllabic signs, *no* and *na* – but these two signs would share the same consonant, *n-*. In the same way, the final sign of 𐀒𐀜𐀰 is likely to share the same consonant as the third sign of 𐀒𐀜𐀯𐀊 and 𐀒𐀜𐀯𐀍. Moreover, it was likely that the inflected endings shared by all these words in fact consisted of the vowel of the penultimate sign plus -𐀊 or -𐀍, and therefore these penultimate signs would also share the same vowel (e.g. the third sign of 𐀒𐀜𐀯𐀊 would have the same vowel as the third sign of 𐀀𐀖𐀴𐀊 and 𐀨𐀍𐀛𐀊). Kober was therefore able to construct the following grid showing the relationships between these signs:

Consonant	Vowel 1	Vowel 2
1	𐀴	𐀵
2	𐀯	𐀰
3	𐀛	𐀜
4	𐀪	𐀫
5	𐀠	𐀡

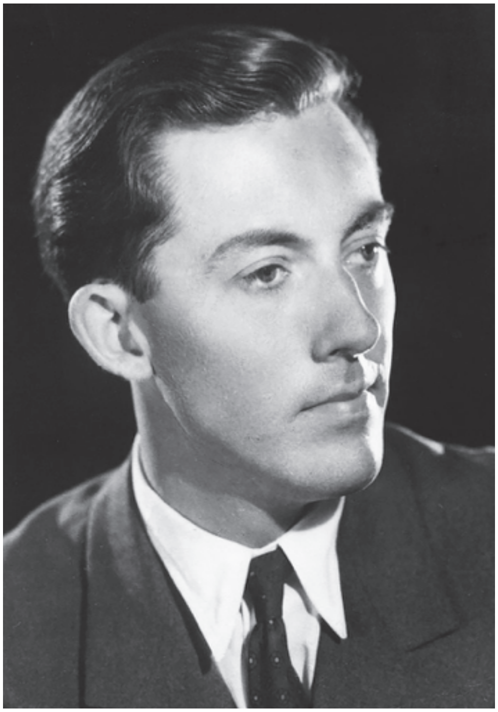


Figure 3
Michael Ventris
(Courtesy of the Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)

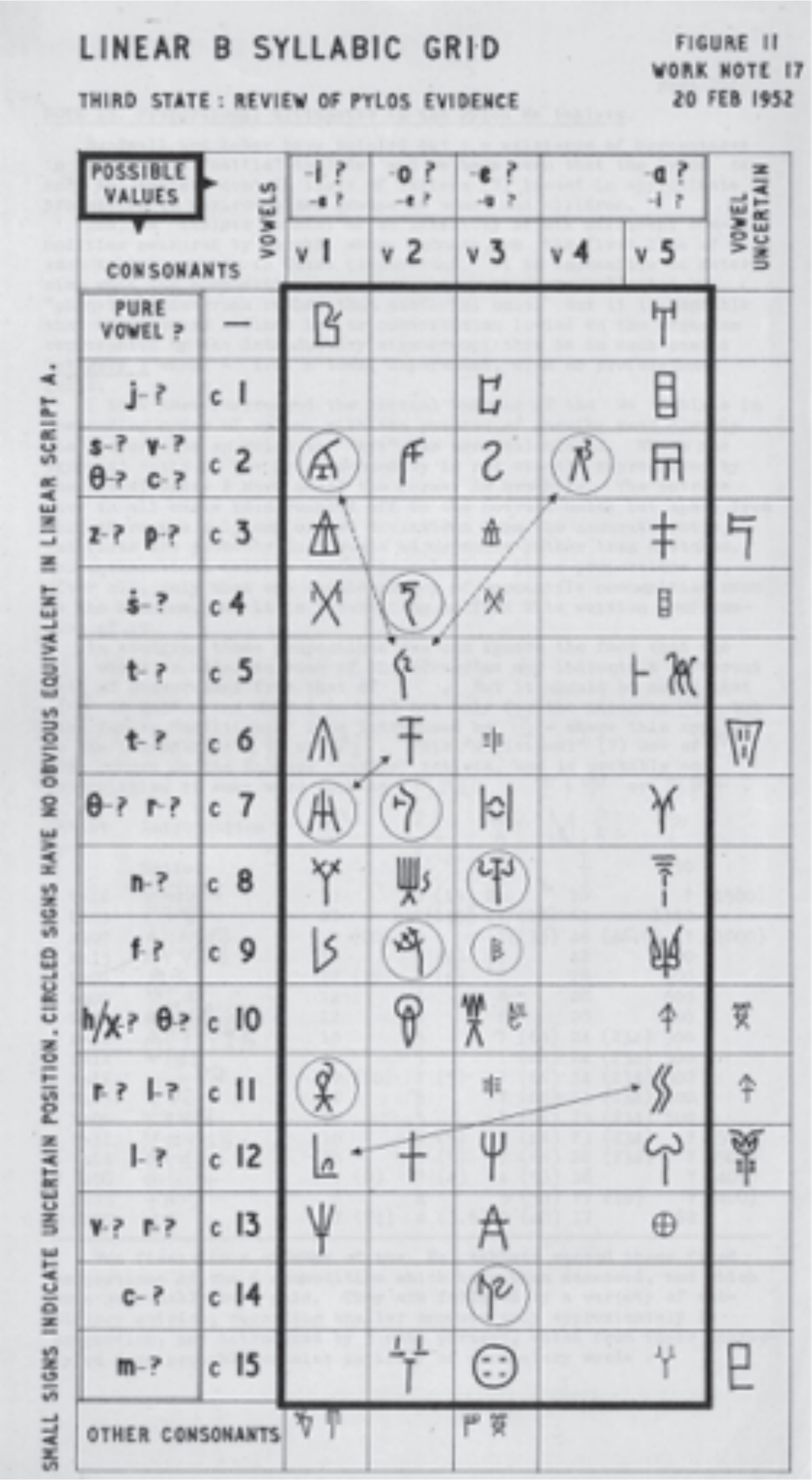
That is, whatever the phonetic value of 𐀴 turned out to be, 𐀵 would have the same consonant as it, and 𐀪, 𐀛, 𐀯 and 𐀡 the same vowel: establishing the sound value of even one sign would therefore immediately provide evidence for the values of other related signs. Kober did not, however, attempt to assign sound values to any of these signs, which she felt there was currently insufficient evidence to do. She concluded the article in which she established this grid by stating that 'when we have the facts, certain conclusions will be almost inevitable. Until we have them, no conclusions are possible.'[8] This grid would ultimately be key to Michael Ventris's subsequent decipherment of Linear B. Sadly, Kober herself would not live to see the decipherment: she died in 1950, probably of cancer, aged just forty-three.

Michael Ventris (1922–56, figure 3)[9] famously became interested in the problem of Linear B after a chance encounter with Sir Arthur Evans on a school trip to a museum exhibition when Ventris was just fourteen.

Unlike Bennett and Kober, Ventris was not a classicist, although he had studied Latin and Greek at school. He trained as an architect, and from 1949 to 1950 worked for the Ministry of Education designing new school buildings. Even in his lunch breaks, however, he continued to tackle the problem of Linear B. His work was carried out in close contact with others working on the script worldwide: in late 1949 he conceived the idea of a survey of the different views among scholars currently working on Linear B about the script's structure, decipherment prospects, and probable language. A questionnaire was circulated to twelve scholars around the world, and the responses, together with his own views, were collected and circulated in 1950 to form what became known as the 'Mid-Century Report'.[10] Kober was one of the few who declined to reply, stating briefly that she considered the questionnaire a waste of time – probably because of its focus on the language of Linear B, which she regarded, with some justification, as at best unhelpful speculation. 'It is possible to prove, quite logically, that the Cretans spoke any language whatever known to have existed at that time – provided only that one disregards the fact that half a dozen other possibilities are equally logical and equally likely,' Kober said in a lecture delivered to the Yale Linguistics Club in 1948.[11]

Although Ventris wrote in the Mid-Century Report that he was 'forced by pressure of other work [i.e. his architectural job] to make this my last small contribution to the problem', giving up his work on the decipherment proved easier said than done; rather, within a year he had given up his job to work full time on Linear B. His methodology was fundamentally based on Kober's identification of groups of inflected words, which Ventris dubbed her 'triplets', and her construction of a grid of related signs: through further detailed analysis, and after the publication of the Pylos tablets increased the amount of material available, Ventris was able to identify many more inflection patterns and other related words, and thus to expand the grid significantly – as well as to begin testing possible sound values for the signs. As he had done with the Mid-Century Report, he recorded and circulated his working in the form of twenty 'Work Notes', detailing the establishment and testing of each hypothesis (figure 4 overleaf).[12] Most of these hypotheses, of course, met with little success – relatively few of the values shown in the grid from Work Note 17 were later proven to be correct. In fact, Ventris was convinced that Etruscan, or a related language, was the most likely candidate for the language of Linear B, and many of his Work Notes are devoted to (unsuccessfully) exploring this hypothesis.

The advantage of the grid system, however, was that it allowed for the testing of any given decipherment hypothesis independent of any suggestion as to the language of the Linear B texts; and eventually, in early 1952, Ventris made a breakthrough with one particular series of hypotheses. It was clear that the sign 𐀀 represented a vowel, rather than a consonant–vowel sign, because of its very high frequency at the beginnings of words (vowels in the middle of words will usually follow a consonant, and so in a syllabic script will be written with a consonant–vowel sign: signs for pure vowels will therefore occur most often at the start of words); he assumed that it might represent *a*. He also assumed, based on similarities with signs in the Cypriot Syllabic script (see above), that 𐀙 was *na* and 𐀴 was *ti*; if those were correct, then the use of the grid meant that he could assign the consonant *n-* to any sign in the same row as 𐀙 and the vowel *a* to any sign in the same column; *t-* and *-i* could likewise be assigned to signs in the same row or column as 𐀴. Thus, the sign 𐀛, which shares a row with 𐀙 and a column with 𐀴, would have the value *ni*, as in the example grid below:



LINEAR B SYLLABIC GRID

THIRD STATE : REVIEW OF PYLOS EVIDENCE

FIGURE 11
WORK NOTE 17
20 FEB 1952

POSSIBLE VALUES	VOWELS	-i ? -e ?	-o ? -e ?	-e ? -a ?		-a ? -i ?	VOWEL UNCERTAIN
CONSONANTS		v 1	v 2	v 3	v 4	v 5	
PURE VOWEL ?	—						
j-?	c 1						
s-? v-? θ-? c-?	c 2						
z-? p-?	c 3						
ś-?	c 4						
t-?	c 5						
t-?	c 6						
θ-? r-?	c 7						
n-?	c 8						
f-?	c 9						
h/χ-? θ-?	c 10						
r-? l-?	c 11						
l-?	c 12						
v-? r-?	c 13						
c-?	c 14						
m-?	c 15						
OTHER CONSONANTS							

SMALL SIGNS INDICATE UNCERTAIN POSITION. CIRCLED SIGNS HAVE NO OBVIOUS EQUIVALENT IN LINEAR SCRIPT A.

Figure 4
An example of the syllabic grid from Ventris's Work Note 17, the last version of the grid to be circulated before the actual decipherment (Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)

Consonant	I	Vowel 2	A
T	𐀴 *ti*	𐀵 *t-*	𐀲 *ta*
2	𐀯 *-i*	𐀰	𐀭 *-a*
N	𐀛 *ni*	𐀜 *n-*	𐀙 *na*
4	𐀖 *-i*	𐀗	𐀔 *-a*
5	𐀪 *-i*	𐀫	𐀨 *-a*

At this point, Ventris made an inspired guess: that the words which featured in Kober's 'triplets', which often appeared in headings on the Knossos tablets, might be place names – and if so, they might correspond to Cretan place names known from later Greek sources. For instance, the harbour of Knossos was called Amnisos during the classical period; in syllabic form, this would be spelt *a-mi-ni-so* (since a syllabic script would have no signs representing single consonants, these would be represented either with a 'dummy vowel', as in *mi* for *m*, or simply omitted, as in the final *-s*). If he had correctly identified the signs for *a* and *ni*, then the word would be 𐀀*-mi-*𐀛*-so*. One word among the group of possible place names seemed to fit: 𐀀 𐀖 𐀛 𐀰; if this really was Amnisos, then 𐀖 would be *mi* and 𐀰 *so*, and the fact that the sign 𐀖 had already been identified in the grid as having the vowel *-i* helped to support this. Another possible place name was 𐀒 𐀜 𐀰, ending in the sign now identified as *so*. Since the other two signs were in the same column of the grid as *so*, they must share the vowel *o*; the second sign was in the same row as *ni*, so must share its consonant, making it *no*. A place name *?o-no-so* was surely *ko-no-so*: the palace of Knossos itself.

Consonant	I	O	A
T	𐀴 *ti*	𐀵 *to*	𐀲 *ta*
S	𐀯 *si*	𐀰 *so*	𐀭 *sa*
N	𐀛 *ni*	𐀜 *no*	𐀙 *na*
M	𐀖 *mi*	𐀗 *mo*	𐀔 *ma*
5	𐀪 *-i*	𐀫 *-o*	𐀨 *-a*

Of course, identifying place names proved nothing about the language itself, since place names are frequently passed on from one language to another – but Kober's 'triplets' provided one further clue. The group headed by 𐀒 𐀜 𐀰, for instance, could now be read *ko-no-so*, *ko-no-si-ja*, *ko-no-si-jo*, interpretable as *Knossos*, *Knossia*, *Knossios*, with the last two words containing the Greek adjectival endings *-ia* and *-ios* and meaning 'woman from Knossos' and 'man from Knossos'. As Ventris continued using the grid to fill in more values and read more of the texts, everything pointed towards a result that he had never expected: the language of the Linear B tablets was Greek. His Work Note 20, dated 1 June 1952 and headed 'Are the Knossos and Pylos tablets written in Greek?', introduced this possibility as a 'frivolous digression', suggesting a few identifications of Greek vocabulary: the words for 'total', for instance, would be *to-so*

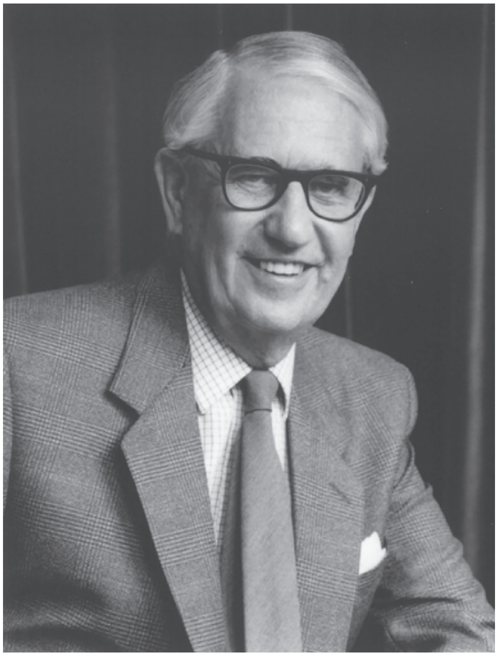


Figure 5
John Chadwick
(Courtesy of the Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)

(probably pronounced *tossoi*) and *to-sa* (*tossai*), corresponding to the masculine and feminine forms of the classical Greek word meaning 'so many'; the words previously identified as 'boy' and 'girl' would be *ko-wo* (*korwos* = classical *koros*/*kouros*) and *ko-wa* (*korwā* = classical *korē*). Although at this stage he still thought that these Greek words 'may well turn out to be a hallucination', this view changed quickly. Just a month later, in a radio broadcast about 'The Cretan Tablets' that he had been invited to present for the BBC (see p. 11), he felt confident enough to announce:

> During the last few weeks, I've suddenly come to the conclusion that the Knossos and Pylos tablets must, after all, be written in Greek – a difficult and archaic Greek, seeing that it's 500 years older than Homer and written in a rather abbreviated form, but Greek nevertheless.[13]

One of those listening to this broadcast was John Chadwick (1920–88, figure 5),[14] a classicist who was just about to start his first lectureship in classical linguistics at Cambridge.

Chadwick had long been interested in Linear B himself, but had not been actively studying it for some time (prior to obtaining his lectureship he had been working on the *Oxford Latin Dictionary*) and so was not among those to whom Ventris had circulated his Work Notes. After listening to the broadcast, however, he obtained a copy of Ventris's work from Sir John Myres, and after just a few days of studying it, he was entirely convinced. Chadwick's knowledge of the history of the Greek language (he was working on a set of lectures on the Greek dialects at the time), combined with his cryptographic experience (like Bennett, he had worked as a cryptographer during the Second World War, breaking Italian and Japanese codes in Alexandria and Bletchley Park; see chapter 6), enabled him to see that Ventris had indeed 'cracked the code' of Linear B. He wrote to Ventris:

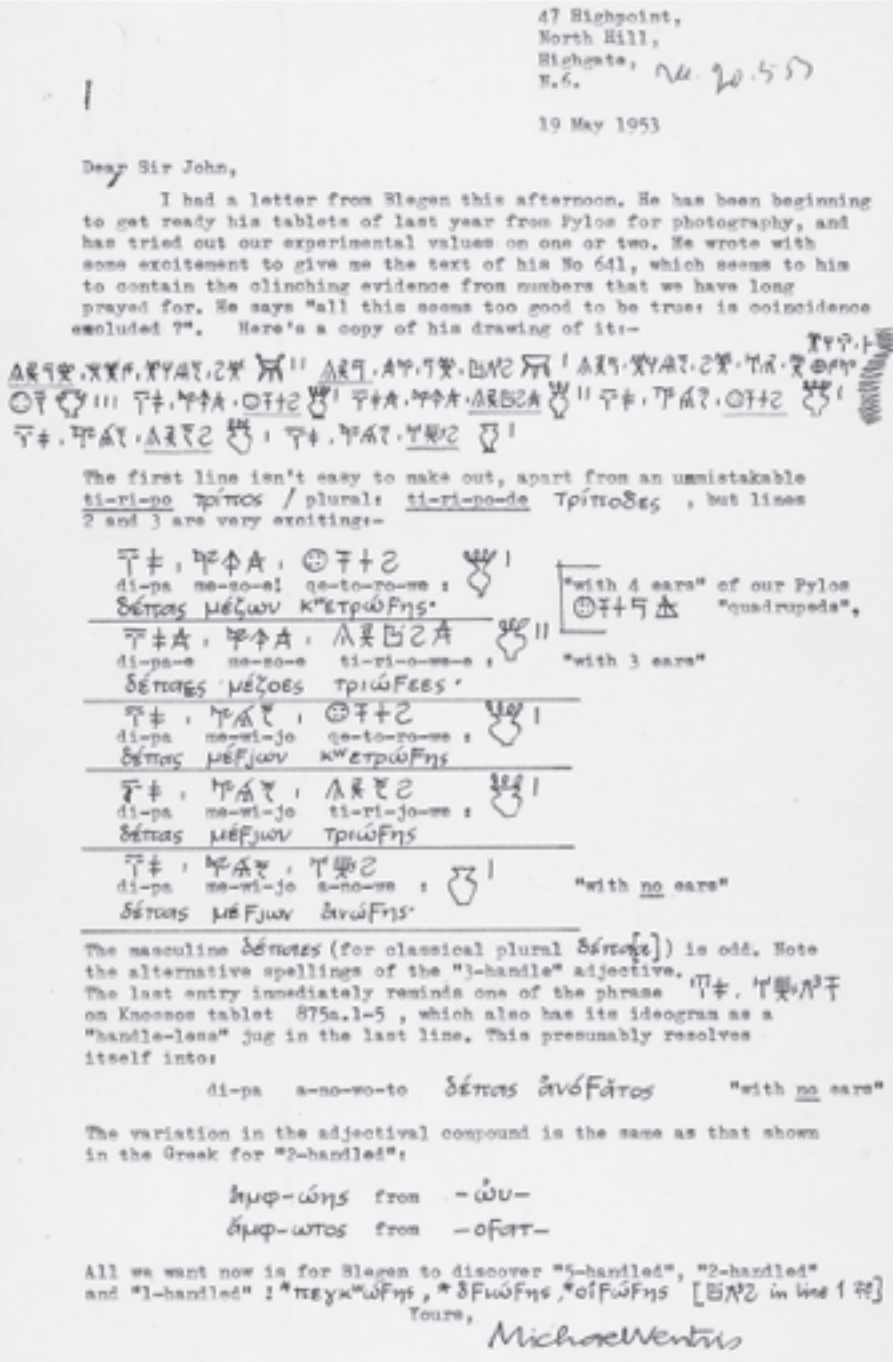
> Let me first offer you my congratulations on having solved the Minoan problem, it is a magnificent achievement and you are yet only at the beginning of your triumph . . . if there is anything a mere philologist can do please let me know.
>
> *Chadwick to Ventris, letter of 13 July 1952*

Ventris wrote back straight away:

> It is very encouraging to hear from someone who has been working on the Minoan problem that they agree with the Greek approach; because frankly at the moment I feel rather in need of moral support . . . I've been feeling the need of a 'mere philologist' to keep me on the right lines.
>
> *Ventris to Chadwick, letter of 13 July 1952*

As a classical linguist Chadwick was able to explain many of the linguistic features of the Linear B texts which were puzzling Ventris, but which were exactly what Chadwick expected for a dialect of Greek that was hundreds of years older than classical Greek. Even in his first letter Chadwick was already able to provide suggestions for interpretations of particular words and identifications of signs to which Ventris had not yet assigned a value: most notably, he (correctly) suggested that the sign 𐀢 had the value *pu* and identified the name of Pylos itself in the tablets from that site.

Thus began a four-year collaboration between Ventris and Chadwick. The following year, 1953, they jointly published the decipherment in an article modestly entitled 'Evidence for Greek Dialect in the Mycenaean Archives'[15] – but after all, the decipherment was so far only a theory. To prove whether it was correct, more evidence would be needed: this was fortuitously provided just a short time later by Carl Blegen, the excavator of Pylos, who was examining a group of tablets which had been discovered the previous year but which had only recently been cleaned to make them legible. Blegen decided to try reading some of the tablets using Ventris and Chadwick's values for the signs. On studying one tablet in particular (now numbered PY Ta 641), he found a remarkable correspondence between the ideograms representing different types of vessels and the undeniably Greek words describing them (figure 6 overleaf): the words *ti-ri-po* and *ti-ri-po-de*, followed by an ideogram representing a three-legged vessel , were clearly *tripos/tripodes* 'tripod(s)'; ideograms showing four, three, or no handles (e.g. , the three-handled pot) were described as *qe-to-ro-we* (*k*^{w}*etr-ōwes*), literally 'four-eared', i.e. 'four-handled'; *ti-ri-jo-we* (*tri-ōwes*) 'three-handled'; and *a-no-we* (*an-ōwes*) 'no-handled'. As an astonished Blegen wrote to Ventris, 'All this seems too good to be true. Is coincidence



47 Highpoint,
North Hill,
Highgate,
N.6. ~~Rec.~~ 20.5.53

19 May 1953

Dear Sir John,

I had a letter from Blegen this afternoon. He has been beginning to get ready his tablets of last year from Pylos for photography, and has tried out our experimental values on one or two. He wrote with some excitement to give me the text of his No 641, which seems to him to contain the clinching evidence from numbers that we have long prayed for. He says "all this seems too good to be true: is coincidence excluded ?". Here's a copy of his drawing of it:-

The first line isn't easy to make out, apart from an unmistakable ti-ri-po τρίπος / plural: ti-ri-po-de Τρίποδες , but lines 2 and 3 are very exciting:-

𐀇𐀞 , 𐀕𐀿𐀁 , 𐀣𐀵𐀫𐀸 I
di-pa me-zo-e qe-to-ro-we :
δέπας μέζων κ^{w}ετρώϝης·

"with 4 ears" of our Pylos 𐀣𐀵𐀫𐀞𐀆 "quadrupeds",

𐀇𐀞𐀁 , 𐀕𐀿𐀁 , 𐀴𐀪𐀃𐀸𐀁 II
di-pa-e me-zo-e ti-ri-o-we-e :
δέπαες μέζοες τριώϝεες·

"with 3 ears"

𐀇𐀞 , 𐀕𐀹𐀍 , 𐀣𐀵𐀫𐀸 I
di-pa me-wi-jo qe-to-ro-we :
δέπας μέϝjων κ^{w}ετρώϝης

𐀇𐀞 , 𐀕𐀹𐀍 , 𐀴𐀪𐀍𐀸 I
di-pa me-wi-jo ti-ri-jo-we :
δέπας μέϝjων τριώϝης

𐀇𐀞 , 𐀕𐀹𐀍 , 𐀀𐀜𐀸 I
di-pa me-wi-jo a-no-we :
δέπας μέϝjων ἀνώϝης·

"with no ears"

The masculine δέπαες (for classical plural δέπα[α]) is odd. Note the alternative spellings of the "3-handle" adjective. The last entry immediately reminds one of the phrase 𐀇𐀞 , 𐀀𐀜𐀺𐀵 on Knossos tablet 875a.1-5 , which also has its ideogram as a "handle-less" jug in the last line. This presumably resolves itself into:

di-pa a-no-wo-to δέπας ἀνόϝᾰτος "with no ears"

The variation in the adjectival compound is the same as that shown in the Greek for "2-handled":

ἀμφ-ώης from -ὠυ-
ἄμφ-ωτος from -οϝατ-

All we want now is for Blegen to discover "5-handled", "2-handled" and "1-handled" ! *πεγκ^{w}ώϝης , *δϝιώϝης ,*οἰϝώϝης [𐀡𐀆 in line 1 ??]

Yours,

Michael Ventris

excluded?' (letter of 16 May 1953). It was; the correspondences were simply too close to be due to anything other than a correct identification of Linear B as representing Greek, and the decipherment was, effectively, proven to all but the most sceptical.

Ventris and Chadwick continued their close collaboration, this time on a book entitled *Documents in Mycenaean Greek*: an ambitious project to publish interpretations of 300 Linear B texts, together with explanations of the decipherment process, the structure of the script, and the evidence it provided for Mycenaean society, which they remarkably completed just three years later in 1956.[16] Both made trips to Greece during this period to study newly discovered tablets: on one such trip to Heraklion in April 1955, Chadwick famously joined two fragments of tablets from Knossos to produce a text reading 𐀂 𐀦 𐂃 – the ideogram for 'horse' following the word *i-qo*, clearly Greek *(h)ikk*^{w}*os* (classical *hippos*) 'horse' – a discovery which went a long way towards convincing the previously sceptical director of the Heraklion Museum, Nikolaos Platon, of the decipherment's correctness. The following year both Ventris and Chadwick attended the first ever international conference on Linear B, held at Gif-sur-Yvette near Paris; a few months later, during one of Ventris's trips to Greece, Chadwick sent him a postcard – written in Linear B – telling him that the manuscript of *Documents* had been sent to the printer. The book would appear in the autumn of 1956, but Ventris never saw it published: a few weeks earlier, while driving late at night, he had been killed when his car collided with a lorry parked in a lay-by. Like Kober, he died tragically young – aged just thirty-four.

After the decipherment: further challenges

Ventris's decipherment and his publications with John Chadwick in 1953 and 1956 were just the beginning: suddenly an entirely new field of 'Mycenaean studies' was opened up, as the Linear B texts provided linguists with the earliest attested stage of any European language, and archaeologists with written evidence of a society previously known only through its material remains. Both Chadwick and Bennett were at the forefront of the development of this new academic discipline, and were instrumental in producing new editions of Linear B texts, in addition to a vast range of other publications relating to the script and the tablets' interpretation. Bennett held posts in classics at Yale, the University of Texas and the University of Wisconsin; Chadwick remained in Cambridge for his whole career, and it is thanks to him that the Faculty of Classics still possesses a large collection of reference and archival materials relating to Linear B, including the letters he and Ventris exchanged between 1952 and 1956. Chadwick also produced a second edition of *Documents in Mycenaean Greek* in 1973, as well as the best-known, and still extremely popular, account of Ventris's achievement, *The Decipherment of Linear B*.[17]

Over the sixty-five years since Ventris's decipherment, intensive study of the Knossos and Pylos tablets, and of those discovered more recently at sites such as Mycenae, Thebes and Chania, has vastly increased our

Figure 6 (opposite)
Letter from Ventris to Myres, 19 May 1953, about Blegen's tripods tablet from Pylos (Courtesy of the Ashmolean Museum, University of Oxford)

understanding of the Linear B tablets and the Mycenaean society by which they were produced (see chapter 3), but of course many questions remain. Perhaps the greatest challenges are the other undeciphered Cretan and Cypriot scripts: even the best-understood of these, Linear A – whose close relationship to Linear B means that we may be able to infer the approximate sound values of many of its signs – is still largely obscure and records an unknown language, while even less is known about other related scripts such as Cretan Hieroglyphic and Cypro-Minoan (see chapter 4). But even the 'deciphered' Linear B is very far from being wholly understood. When Ventris made his announcement on the radio, he had actually assigned sound values only to around two-thirds of the script's syllabic signs, and although this number was increased significantly by his, Chadwick's, and others' subsequent work, fourteen Linear B signs – around a sixth of the syllabary – still remain 'undeciphered', their sound values unknown or uncertain. In most cases, the status of these (generally rare) signs is unlikely to change unless further examples are found to provide evidence as to their values.

Even when a tablet can be read in its entirety, its content may still remain obscure if its terms cannot be identified with known Greek words; and even where texts can be fully translated, their laconic nature makes them likely to raise as many questions as they answer. Consider this entry in lines 5 and 6 of a land-holding tablet at Pylos (PY Ep 704, figure 7), one of the relatively few complete sentences attested in the Linear B texts:

𐀁𐀪𐀲 𐄀 𐀂𐀋𐀩𐀊 𐄀 𐀁𐀐 𐄀 𐀁𐀄𐀐𐀵𐀤 𐄀 𐀁𐀵𐀛𐀍 𐄀 𐀁𐀐𐀁 𐄀 𐀳𐀃 𐄀 𐀅𐀗𐀆𐀖 𐄀 𐀞𐀯 𐄀
𐀒𐀵𐀙𐀃 𐄀 𐀐𐀐𐀕𐀙𐀃 𐄀 𐀃𐀙𐀵 𐄀 𐀁𐀐𐀁

e-ri-ta , i-je-re-ja , e-ke , e-u-ke-to-qe , e-to-ni-jo , e-ke-e , te-o , da-mo-de-mi , pa-si ,
ko-to-na-o , ke-ke-me-na-o , o-na-to , e-ke-e

Erit^{h}a (h)iereia (h)ek^{h}ei euk^{h}etoi-k^{w}e etōnion (h)ek^{h}ehen t^{h}e(h)ōi dāmos de min p^{h}āsi ktoināhōn k^{h}ek^{h}emenāhōn onāton (h)ek^{h}ehen

Eritha the priestess has and claims to have an *etōnion* [landholding] for the god, but the local authority says she has a lease of public[?] land

Clearly, a 'legal' dispute of some kind is going on: Eritha has been allocated some land to use, but she and the local administrative body (the *dāmos*) who assigned it to her now disagree on the nature of her allocation – she claims it to be an *etōnion*, a term whose precise meaning is unclear but which obviously refers to a more advantageous landholding arrangement than the 'lease' (*onāton*, literally 'benefit') the *dāmos* claims she has. From this entry, and other similar entries recording land allocations, we can extract a good deal of information about Mycenaean Pylos: the people and authorities who controlled the allocation of land, and the people who received it from them; the economic position of religious personnel (Eritha holds her land 'for the god' in her capacity as priestess); even the

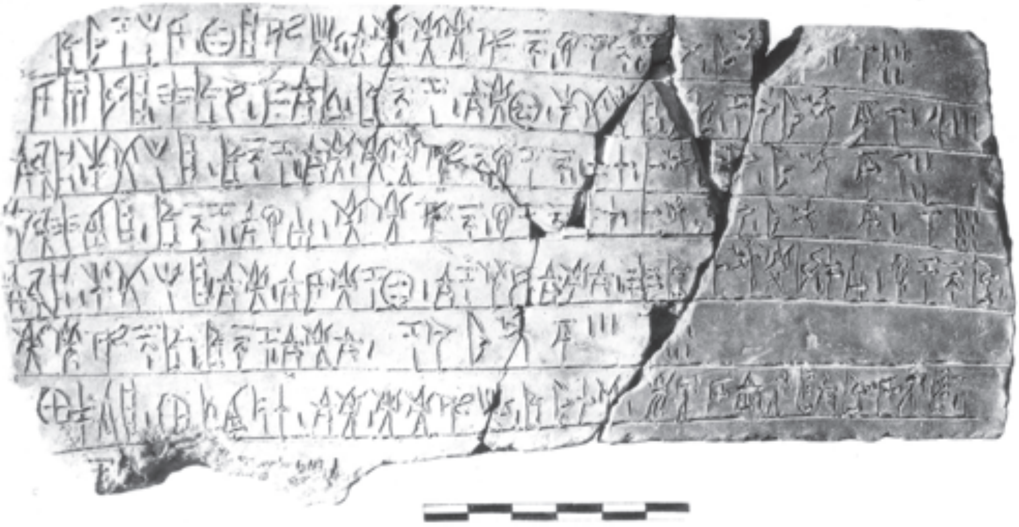


Figure 7
A land-holding tablet (PY Ep 704) from Pylos containing a 'legal' dispute
(Courtesy of the Department of Classics, University of Cincinnati)

social position of women, who rarely appear as high-status individuals in the tablets except in religious roles, as here. And yet there are so many questions that this text, which is ultimately concerned mainly with recording the quantity of land in question, does not answer: why did the dispute arise? Was it all a misunderstanding, was the *dāmos* trying to cheat the priestess, or was Eritha out to get a better deal for herself? Who was responsible for resolving such disputes, and how did they do so in this case – or was the issue still ongoing when the destruction of the palace preserved this tablet for archaeologists to find three millennia later? Such questions may never be answered, but that we can even begin to ask them is due to the work of all those who contributed towards Linear B's decipherment and subsequent study. The decipherment of Linear B not only 'cracked the code' of the script, but in doing so turned the tablets into a unique – and tantalizing – window into the Mycenaean world.

3

Reading Between the Lines: The Worlds of Linear B

John Bennet

On 1 July 1952 our approach to the study of ancient Greece changed definitively: on that day Michael Ventris announced to the world on BBC radio his proposed decipherment of the Linear B script, a script that had for over a half century defeated many scholars, not least Sir Arthur Evans, excavator of the site of Knossos, who had named it (see chapter 1). Prior to the decipherment scholars were dependent on archaeological data. Moreover, the excavations of Heinrich Schliemann in the later nineteenth century had established the principle that the Homeric texts (the *Iliad* and *Odyssey*) contained reminiscences of the Late Bronze Age Aegean, usually referred to as the 'Mycenaean' period. A minor consequence of this was the naming of key sites after figures from Greek legend, for example, the palaces of Minos at Knossos or of Nestor at Pylos; a major consequence was a rather reductive view of Mycenaean society.

The decipherment fundamentally changed the situation, but the existence of readable texts did not automatically transform this period into a historical one. The Linear B texts are both limited in time reference and relatively small in number: just over 6,000 in total, against the hundreds of thousands known from the albeit much larger Mesopotamian cuneiform world that stretched from Iraq to Turkey and spanned three millennia. Their preservation depends on burnt contexts, often assumed to be destruction levels, in archaeological sites because they were not deliberately baked, but written on damp clay then allowed to dry. The documents therefore belong to a single administrative season and offer no time depth; they are 'synchronic', rather than 'diachronic'. Finally, they were written not for posterity, but for a very limited audience who could read and write the script. Behind the relatively telegraphic inscriptions, therefore, lie the contexts in which they were produced and the purposes for which they were written. The anonymous people who wrote the documents – we call them 'scribes' – fully understood both context and purpose; we do not.

This chapter focuses on how the decipherment opened up the social and economic world of Late Bronze Age or Mycenaean Greece to modern scholars. My broad theme is to highlight the contributions the texts have made to expanding our knowledge, emphasizing how important it is to read between the lines of text and between documents to reconstruct both context and purpose. Here archaeological data are crucial, both on the micro level, allowing us to see which texts were physically associated with one another and where they were found within sites, and on the macro level in reconstructing the wider material world in which people lived at the time. The fact that examples of writing are confined to a small number of sites and, within those sites, to a small number of rooms helps us appreciate how tiny was the community of 'administrators' in Linear B; the vast majority of those living at the time must have been either illiterate or have had no use for the script, even if they came into contact with palatial administrators.[1]

Contexts and purposes

Given both the ubiquity of material evidence and the rarity of Linear B texts, the archaeological context is of considerable importance. Yet that observation does not diminish the value of being able to read (and largely understand) a series of administrative documents spanning about two centuries in the Late Bronze Age (about 1400–1200 BC) from places in Crete (e.g. Knossos, Chania) and mainland Greece (from Pylos and Ayios Vasileios in the southern Peloponnese, through Mycenae and Tiryns in the north-east Peloponnese, to Thebes and Volos in central Greece, see the map on p. xvi). In addition to the administrative documents, there are almost 200 transport vessels, known as stirrup jars, painted with Linear B inscriptions before firing and attested at most of the above sites and a handful more within the Aegean. The stirrup jar is the trademark Mycenaean transport vessel, examples of which, most not inscribed, are plentiful in excavations.[2] They are attested at most of the above sites and a handful more within the Aegean, were inscribed in Linear B before firing.

The material world of Mycenaean Greece documented through archaeology is rich and, unlike the world of the Linear B texts, has considerable time depth. However, that world is fragmentary: many materials survive archaeologically, but others do not. Ceramics are, of course, ubiquitous – breakable, but virtually indestructible – but other materials also survive: including metals (bronze, lead, silver, gold), stone, ivory, glass and faience. In the case of valuable materials, especially metals which could be recycled, our ability to recover them depends on their deliberate deposition in contexts that have remained undisturbed to the present, such as tombs, sanctuaries or hoards; the archaeological record, though full, is also skewed by pre-depositional and post-depositional factors. As material objects recovered archaeologically the Linear B texts are themselves also subject to these factors.

Many of the Linear B documents were written as part of the process of acquisition or production of materials, objects or commodities for consumption or exchange by the central authorities we conventionally refer to as 'palaces'. Although our documents are themselves archaeologically rare, unlike archaeological materials, they contain data on quantities. Obviously we have nothing like a complete inventory of any single material at any single site, but it is of some value in appreciating scale to

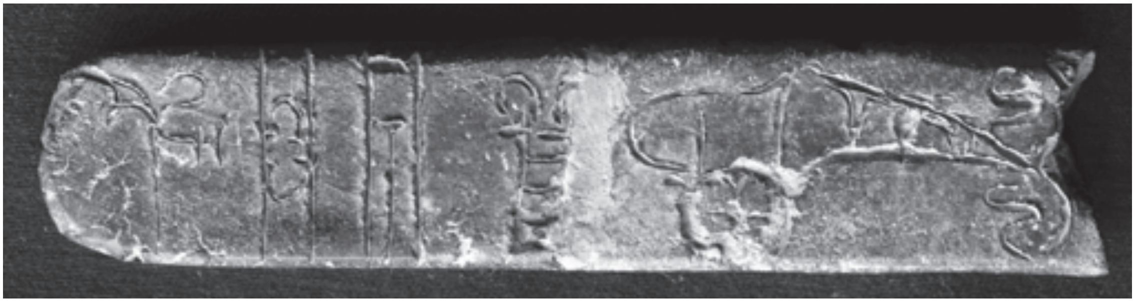
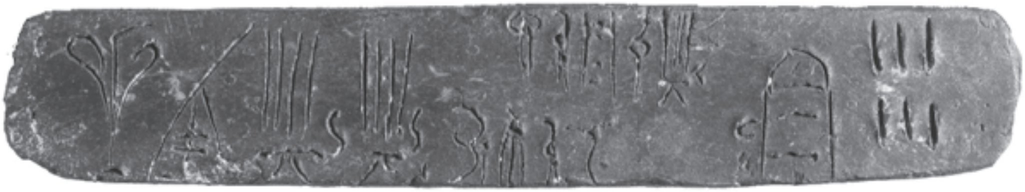


Figure 1
Linear B document (Sc 238) from Knossos, showing armour and one of over a hundred chariots recorded in this series of texts (Ashmolean Museum, AN1938.704. Courtesy of the Ashmolean Museum, University of Oxford)

know, for example, that a document was produced at Knossos (K 700) that recorded 1,800 transport stirrup jars, perhaps a single 'order' placed by the palace for containers to accommodate a shipment of oil or wine. Each had a capacity of about twelve to fourteen litres; this number would accommodate as much as 25,000 litres of oil or wine. We can also, for example, total up the numbers of chariots recorded at Knossos (over a hundred in one early set of documents (figure 1); at least thirty, all elaborately decorated, in a later set, stored at Knossos and also at three other key sites, including Chania and Phaistos) or the number of bronze workers listed as available (perhaps 300) to the palace-centre of Pylos to work 576 kilogrammes of allocated bronze. Similarly, by identifying their individual handwriting, we can suggest that there were about thirty scribes working at Pylos at the time the documents were preserved, perhaps twice as many at Knossos (although the complexity of the chronology of the Knossos documents makes it difficult to total up the scribal workforce at any one period).

Such quantitative information helps us understand scale of production or use. But not all materials survive archaeologically and here the texts can help substantially. Although we can recognize containers that might have contained oil or wine, those substances themselves are not preserved, even if our ability, through archaeological chemistry, to identify what vessels had actually contained is constantly improving. What the texts can tell us about oil, however, is something about its *quality*, as well as about quantities: that it was perfumed at Pylos by the addition of various plant materials, for example sage, rose and cyperus (sedge). The scale of the industry at Knossos also becomes clear from the stirrup jars already mentioned, and also from a series of texts documenting thousands of litres of oil entering and leaving the palace; a totalling document notes over 9,500 litres of oil. Production seems to have been centralized at Knossos

Figure 2
Linear B document (Ga [1] 676) from Knossos showing a delivery of coriander (Fitzwilliam Museum, GR.1.1911. Courtesy of the Fitzwilliam Musuem, University of Cambridge)



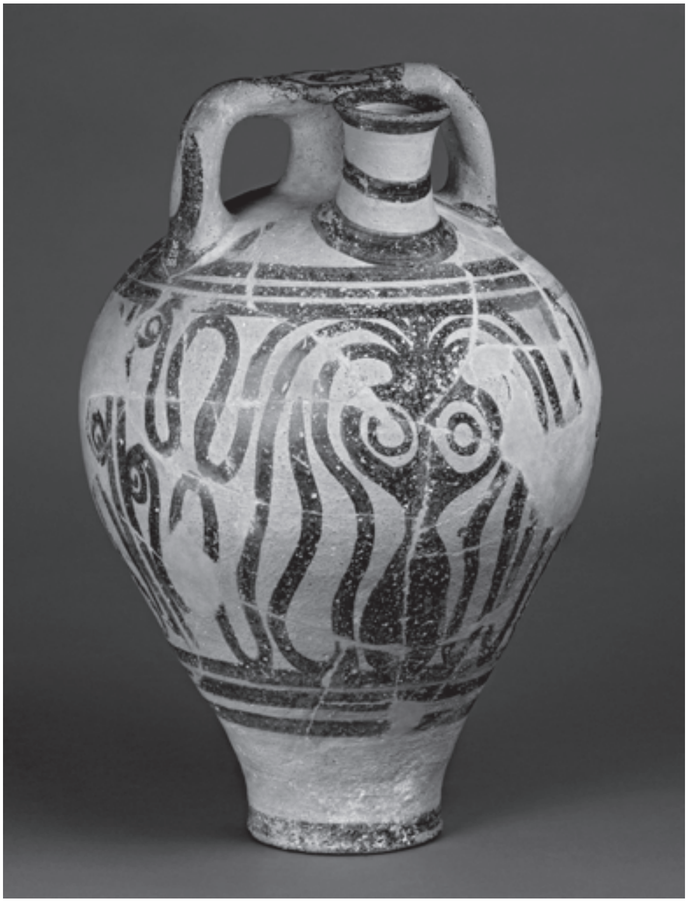


Figure 3
Stirrup jar for transporting oil or wine from Episkopi-Bamboula, Cyprus (British Museum, 1896,0201.265. Courtesy of the Trustees of the British Museum)

itself, oil and scent ingredients (like coriander and the mysterious *po-ni-ki-jo*, perhaps a colourant as well as a scent) being delivered separately (figure 2).

The scale of production fits with a general picture in which such perfumed oil products were prized in the markets of the eastern Mediterranean world, where their aromas (in a world without modern western standards of hygiene) were associated with the divine and also the elite, who could afford them. The shape and characteristic octopus decoration of these jars presumably signalled the origin of the oil or wine they contained, rather like modern wine bottles (figure 3).[3] When such vessels travelled *within* the Aegean, they sometimes bore Linear B inscriptions, painted before firing, so part of the vessel's manufacturing process before it was filled. These inscriptions included minimally a personal name, sometimes also a Cretan place name, on occasion the term 'royal' (*wanaktero-*) and perhaps indicated the manufacturer of the vessel.[4]

Another finished product much prized in the eastern Mediterranean world of commodities was cloth. Here the existence of several series of documents from Knossos transformed our appreciation of these

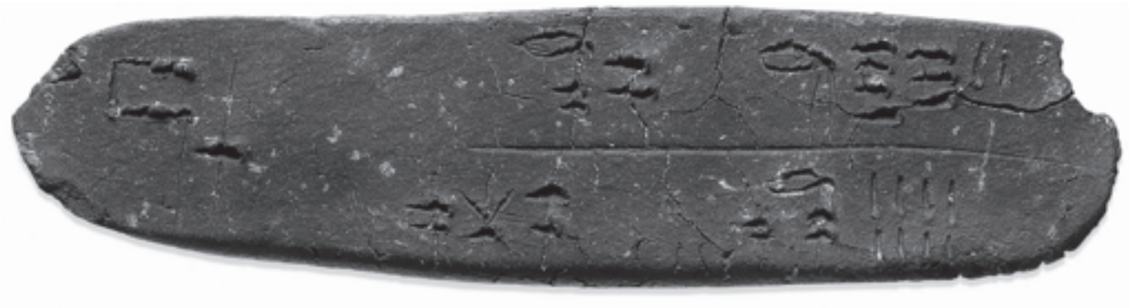


Figure 4
Linear B document (Dd 1171) from Knossos, one of 600 flock census records, in this case documenting a flock of a total of a hundred sheep at the site of Phaistos (the name appears in the middle of the bottom line) in south-central Crete (British Museum, 1910,0423.2. Courtesy of the Trustees of the British Museum)

Aegean products. Textiles are extremely rare as archaeological finds in the Aegean, their preservation dependent on very specific circumstances, often mineralization in proximity to nearby metalwork. We therefore have to reconstruct their appearance indirectly through representations, mostly on palatial wall-paintings.[5] Even then, such interpretations tell us little of the process of production, let alone the quantities involved. The Knossos documents, first studied and presented by John Killen,[6] reveal a chain of production from the management of over 80,000 sheep in over thirty locations, recorded by a single scribe on 600 tablets (figure 4), through their shearing to provide wool, which was assigned to at least 900 female weavers, supported with rations of grain and figs from palace-controlled stores, at workshops in about fifteen different locations across much of Crete from the Rethymnon to the Lasithi regions. Different weights of cloth were produced, which were also dyed (purple, red and yellow are attested), 'finished' by the addition of embroidered details or edging ('white' or 'multicoloured'), for example, and ultimately ended up in storage at the palace of Knossos itself, where again texts identify certain bundles of cloth as probably 'for export' or 'for the "followers"' – a high-status group within the Mycenaean elite. The surviving storage documents list at least 190 pieces of cloth.[7] The presence of finished cloth 'for export' suggests that Knossos must have been a major player in the eastern Mediterranean textile trade, contributing its trademark products to an international market. Unfortunately the Linear B texts are all but silent on the process of trade itself. Two documents from Pylos appear to record a payment (*onos*) from palace stores for a delivery of alum (*struptēria*). The commodities offered are varied, including wool, goats, wine, tunics and figs, but no equivalence is stated, as is consistent with transactions throughout the documents.

Without the texts we would have little concrete data about the extent of this industry, involving so many sheep and such a large, dedicated workforce. Another important contribution is to show that production of textiles took place at a number of locations throughout much of central and west central Crete as part of a unified production programme ultimately managed from Knossos, the ultimate destination of the products. Had we been fortunate enough to encounter multiple, contemporary textile workshops in excavations at many sites across the region, we might well have interpreted these as workshops producing for that particular community or for trade by that community. However, we should not fall into the trap of interpreting the texts over literally; it would be easy, for example, to read these documents as revealing total control by the palace authorities at Knossos over much of the sheep population of this region of Crete. However, for various reasons discussed by Paul Halstead[8] and others, it appears that the palace was in fact claiming the rights to the wool clip from certain flocks through contracts with those flocks' owners, whom we conventionally call 'shepherds'; the flocks themselves were probably made up to nominal round figures annually from other animals owned by these individuals. The female workforce was supported – in those locations, not centrally at Knossos – in its work on palace textiles by rations mobilized by the palace. What these women did at other times was not documented by the palace. A similar situation obtained in the Pylos polity, across which there were some 750 female workers distributed at around sixteen places. In this instance, probably some 150 years later than the situation at Knossos, the majority of these workers (perhaps 450) were located centrally at Pylos itself.

So although Knossos maintained quite detailed records and was the ultimate destination of the finished product, the system drew on only a portion of the local resources (of animals, wool and labour). The integrity of the system was monitored through a system called *talasía* in Mycenaean Greek, derived from 'talent', a denomination of weight: wool was distributed to workshops with a target of so many pieces of cloth to be produced of different type, based on the weight of wool involved. A similar system was used in the Pylos bronze industry, where the 'smiths' contracted to the palace to work bronze into finished artefacts were described as 'having a *talasía*', or 'without one' (*atalasio-*), and the raw material was distributed by weight. Chariot wheels also came under the same regime. There are parallels for this mode of production further east in Levantine and Mesopotamian societies, where it was known by the Akkadian term *iškāru*.

Not all palatial production was managed in the same manner. The production of oil – once acquired by the palatial centre – was difficult to manage in this way, since, by definition, the ingredients other than oil (essentially those elements that gave the oil its scent) were consumed in the process of production. Here the texts document oversight by high-level palatial employees and specialists referred to by the term 'unguent-boiler' (*a-re-pa-zo-o*); for example, a Pylos text documents the delivery of ingredients for perfumed oil by a high-ranking official (Alxoitas), one of the 'collectors' at Pylos, to an 'unguent boiler'.

Not all materials were acquired by the palaces through multistage management of production from raw materials. Like pottery, grains, for example, were probably mostly requisitioned as products, rather than grown on palace estates, although some Knossos texts suggest that palace-owned oxen might have been allocated to assist with cultivation (figure 5 overleaf).[9] Some materials were acquired as finished products through a process of 'taxation' on subordinate communities. The Pylos Ma-series

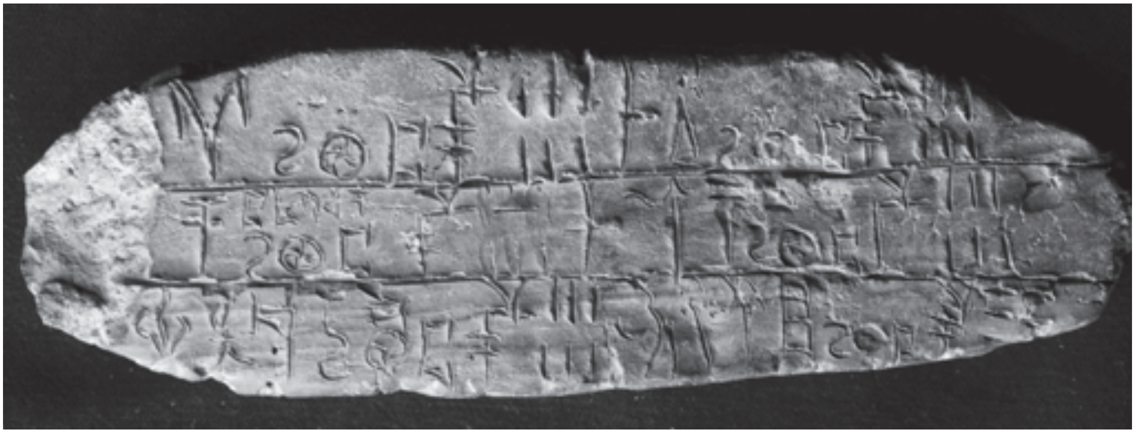
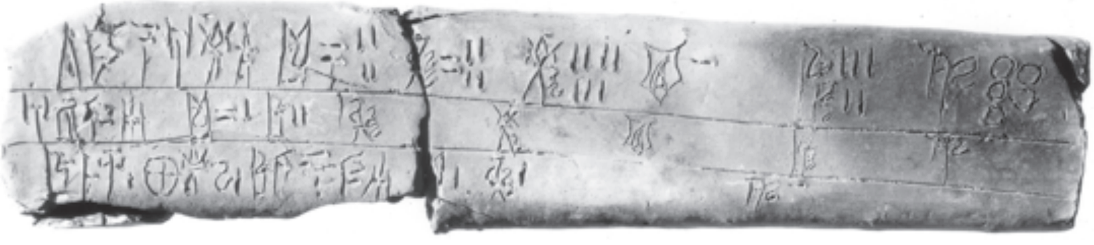


Figure 5
Linear B document (Ce 59) from Knossos, listing 'working' oxen at six locations in central and western Crete, including Tylissos and Chania (Ashmolean Museum, AN1910.212. Courtesy of the Ashmolean Museum, University of Oxford)

texts document this most completely, although a similar series at Knossos appears to document the same process there. A single document exists for each of the seventeen districts at Pylos, each listing an assessment of six commodities, not all of which we can securely identify, but certainly including a simple type of cloth (possibly a tunic known as a *wehanos*) and ox hides, perhaps also linen thread and beeswax (figure 6). The commodities appear in a fixed ratio to one another, but the absolute quantities vary by district, probably in relation to their productive capacity. Because the commodities are demanded from every district, they are apparently not environmentally sensitive. There are three types of documents, but only one type exists per district: a plain assessment, an assessment with a delivery noting shortfalls, or an assessment indicating missing quantities from a previous year, each with declared exemptions for specific groups, such as 'smiths'. These documents imply an administrative process: the plain assessment documents would be replaced by receipt documents as deliveries came in. It is possible that the commodities were required for the manufacture of military equipment, but the fact that every community was required to produce them, and in a fixed ratio, suggests a symbolic as much as a practical rationale: a statement of power from the centre.

Other production practices were, it seems, more exclusive to the palace, and were described by specific terms, perhaps coined within the palatial sphere.[10] 'Unguent boiler' is one, but others were formed using a suffix (*-worgós*) connected to the English word 'work', such as '(blue) glass workers' (*kuwanoworgoi*) or 'gold workers' (*khrusoworgoi*). Although the word 'ivory worker' is not (yet?) attested, a tablet from Pylos, rather similar in purpose and content to the oil distribution tablet mentioned above and involving the same official, Alxoitas, documents the distribution of two tusks for further working. This type of production seems to have depended on a monopoly by the palaces in the supply of the raw materials (gold, glass, ivory), which were then worked by specialists within the palace complexes and only became visible as finished products, such as the moulded glass beads widely attested in subelite tombs, or the composite products, combining wood, stone, ivory, gold and glass rarely preserved



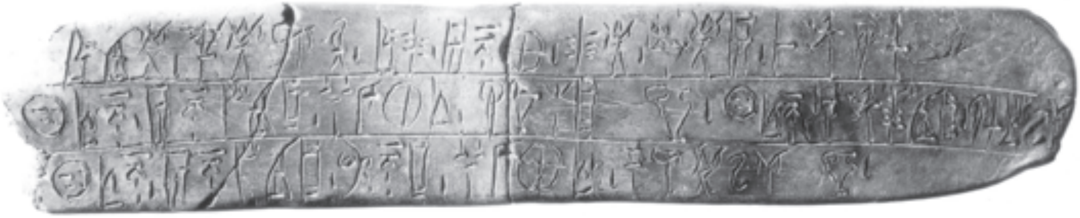
whole archaeologically, but displayed at palace-sponsored events, as we know from a particular set of Pylos texts, the Ta-series.

The famous 'tripod tablet' that played an important role in confirming the decipherment (see chapter 2) was one of this group of thirteen tablets that contains descriptions of over seventy objects collected for use on the occasion of a sacrificial banquet to mark the royal appointment of a man called Augewas to the office of *da-mo-ko-ro* (figure 7). The equipment includes six bronze tripod cauldrons, other metal vessels, and equipment for the sacrifice and preparation of the animal(s) for the banquet. Most striking are eleven tables, six ornate, high-backed chairs and sixteen footstools. The tables are made of stone or wood, the other furniture of wood, inlaid with valuable materials like gold and blue glass, but mostly with ivory, carved or engraved with various designs such as palm trees, helmeted heads, spirals or shells.[11] The specific meaning of some of the terms for decorative motives stubbornly eludes us and is a salutary reminder of how difficult interpretation of Linear B can be when based solely on lexical items with no visual or archaeological context. Many of the terms, like those mentioned above, are clear enough and well known in actual examples of ivory plaques, inlays or vessels recovered archaeologically, but convincingly matching others to the large range of other attested motives is challenging. That said, without these texts, we would have difficulty visualising the quantities and the types of material culture mobilized by the Mycenaean palatial elite on such an occasion.

The Ta tablets just described do not list the food consumed on this particular occasion, but others do for other events, further enhancing our grasp of royal ceremony at Pylos and giving an impression of its scale.[12] One document, for example, lists the 'menu' for a banquet marking the king's 'initiation', perhaps his coronation, which includes one ox (that could have produced around a hundred kilogrammes of meat), plus forty-three other animals (sheep, goats and pigs) and just over twenty units of

Figure 6
Linear B document (Ma 123) from Pylos, listing an assessment for six commodities (top line: tunics, linen thread (?), beeswax (?), ox hides and two other unidentified), a delivery (middle line) and exemptions (bottom line) for the place known in Linear B as 'ti-mi-to-a-ke-e', probably the site of Nichoria
(Courtesy of the Department of Classics, University of Cincinnati)

Figure 7
Linear B document (Ta 711) from Pylos introducing a set of thirteen documents listing equipment for a sacrificial banquet, including the jugs (qe-ra-na) listed here on the second and third lines
(Courtesy of the Department of Classics, University of Cincinnati)



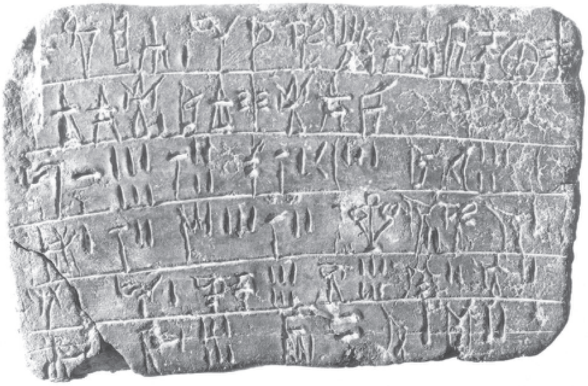


Figure 8
Linear B document (Un 2) from Pylos listing the supplies for a banquet at the place Sphagianes, near Pylos, on the occasion of the king's 'initiation'; the ox appears one entry in on the penultimate line followed by sheep, goats and pigs, with wine noted almost exactly in the middle of the last line (Courtesy of the Department of Classics, University of Cincinnati)

wine (equivalent to around 580 litres) (figure 8). Study of archaeological deposits of animal bones by zooarchaeologists can tell us a great deal about the species consumed and the mode of consumption, but archaeological deposits cannot be linked to any specific textually attested event; nor can they confirm how many animals were mobilized for consumption on a particular occasion, or the nature of the occasion itself. Archaeological study of bones can, however, add to the textual information insights into butchery practice and cooking techniques, including burnt sacrifice, effectively telling us about palatial 'cuisine'. At Pylos at least, cached remains recovered archaeologically of animals consumed on such occasions confirm the importance of oxen (despite the broader range of species listed), while their deliberate deposition in specific locations around the palace further emphasizes the significance of such events as implied by the texts. The picture that emerges through combining multiple sets of evidence is of banquets catered at some scale and as a multisensory experience, engaging sight, smell, touch, taste and hearing. Pylos wall-paintings suggest sung performances accompanied these events, but no poetic texts are known in Linear B, despite the wishful thinking when the documents first came to light, and even after the decipherment, of scholars who hoped to find a predecessor to Homer's *Iliad* or *Odyssey*. It appears that this aspect of Mycenaean elite culture remained oral. A small consolation is the recording of two 'lyre players' among a list of people on a tablet from Thebes.

Political geography and social organization

One of the keys in the decipherment was the identification of place names like Knossos and Amnisos (see chapter 2). Where place names mentioned in the texts can be associated with particular places in the landscape, this can help us to understand the geographical extent of the Mycenaean polities. So, among the Knossos texts, six place names can be securely identified with sites known in later sources by those names: Knossos itself, Amnisos and Tylissos, nearby to the north-east and west respectively, Phaistos in the Mesara plain to the south, and Kydonia (modern Chania) and nearby Aptera in the far west of the island.[13] This implies a total area for the Knossos polity of around 2,700 square kilometres, an area not much larger than the English county of West Yorkshire (2,029 square kilometres).

Many place names, however, some clearly of significance because of their frequency of occurrence or the quantity of materials or activity attributed to them, cannot be identified in this way. The Pylos texts contain many of these; in fact, only Pylos is certainly identified and ironically not in the same location as either classical or modern Pylos. The geographer Strabo, writing in the Roman period, notes the tradition that an older Pylos lay 'under' a mountain called Aigaleon and the Pylos texts contain references to a division of the polity into two provinces, 'this side of' and 'beyond' Aigolaion. Although not an exact match, it is difficult not to identify this term with Strabo's Aigaleon and the actual ridge that rises prominently a few kilometres east of the palace at Pylos. Here texts of different genres and dates, plus local topography, combine to offer an interpretation. Linear B scholars refer to these two parts as the Hither ('this side of') and the Further ('beyond') Provinces. Moreover, three documents list a set of place names in a fixed order, nine in the Hither, seven in the Further Province. The seventeen Pylos Ma-series tablets, one for each district, imply that there might have been eight Further Province districts.

Among the Thebes tablets, Thebes itself and nearby Eleon (known in Homer) appear, as well as two places on the island of Euboea (Amarynthos and Karystos). Provided that these place names have not moved in antiquity, as was the case with Pylos, for example, their appearance in the archive implies that palatial interests of Thebes extended across the narrow straits to that island, something that would not have been obvious without the texts. It is somewhat frustrating that no useful geographical terms appear among the small number of texts known from Mycenae or Tiryns, since these might help us to understand how two large, fortified citadels co-existed in such proximity in the thirteenth century BC. Equally, we do not know whether the territories surrounding each palatial centre had fixed boundaries or whether control was uniform within those boundaries. We can note, for example, that detailed records of land tenure, such as those attested from Pylos, seem to be confined to areas close to the centre itself. It is also of interest that land was measured in 'seed' grain, not an absolute measure of area, a practice also known in later land regimes, such as that of Ottoman Greece.

There are also tantalizing references in some document to areas probably outside each polity. At Thebes there are references to individuals from Lakedaimon, presumably the region in which the classical city of Sparta lay, implying some form of connection to the southern Peloponnese. Similarly, among the 750 or so female workers documented at Pylos, there are groups referred to collectively by terms implying their origin in the eastern Aegean: Chios, Cnidos, Halikarnassos, Lemnos and Miletos, plus Kythera, an island just off the Laconian coast, so somewhat closer to Pylos itself.

The Linear B documents contain no descriptions of the political order of the state that produced them. That inequality existed is clear, of course, from the archaeological data – palaces, as against smaller settlements, or different types or sizes of built tombs, for example. A more nuanced picture is possible from the texts, but inferring it requires reading between the lines and interpretation of the usage in the Late Bronze Age of terms known in later Greek. By analogy with later usage of terms that appear in Linear B, we can reconstruct something of the political hierarchy. The term *wanax* (Linear B *wa-na-ka*; later Greek ἄναξ) occurs in documents in at least three sites (Pylos, Knossos, Thebes and, possibly, Chania). In Homer and most historical dialects of ancient Greek this term, perhaps best translated as 'lord', had moved into the divine sphere, applied to deities. The contexts in which the term *wanax* occurs in Linear B suggest it was the title of the head of the Mycenaean state, the 'king'. So, the *wanax* appoints an official in the heading tablet for the Ta series mentioned above and has a banquet in his honour (figures 7 and 8). No other named or titled individual behaves or is honoured in this way. A single text (Er 312), recording plots of land (*temenos*) assigns a plot three times larger than the next largest to the *wanax*. Similarly, produce and products could be labelled 'royal' (*wanaktero-*), such as certain pieces of cloth at Knossos and probably some of the oil in transport stirrup jars. The term is also applied to some craftspeople (a potter, an armourer, and a fuller), listed as holding land, perhaps in exchange for acting as craftspeople 'dedicated' or 'attached' to the office of *wanax*. Although not universally agreed among specialists, it is possible that the man who bore the title *wanax* also appears in other contexts in the Pylos texts under his own name (Linear B *e-ke-ra$_2$-wo*, perhaps *Ekhelawon*), here acting as a member of the elite rather than as head of state. The Greek word for 'king' in later Greek (βασιλεύς) appears in Linear B (as *qa-si-re-u*) both at Pylos and Knossos. Instead of referring to a single figure, as usually in later Greek, in Linear B this term refers to multiple individuals – unlike the *wanax*, always mentioned in the singular – in some cases associated with craft production. It seems that this term has been elevated in later Greek, while the term *wanax* has shifted register from the secular to the divine.

The same land-tenure document just mentioned also lists the *temenos* of a figured called the *lāwāgétās* (Linear B *ra-wa-ke-ta*), attested at Pylos and Knossos, but much rarer in later Greek (it occurs in poems by the early fifth-century BC poet Pindar). The term can be interpreted etymologically as 'leader of the *la(w)os*', perhaps in the sense of 'host', that is a military force. That this figure ranks second to the *wanax* in the land holdings recorded here implies considerable status, as does the fact that another land-holding document refers to at least one craftsperson (a chariot fitter) 'dedicated' to his office (*lawagesios*) (figure 9). There is little else to go on in interpreting his role, although many scholars agree on the idea that he was second-in-command in the Mycenaean state, perhaps with a military role, the complementary distinction between his office and that of the *wanax* perhaps reflected in the opposed adjectives *wanakteros*, as opposed to *lawagesios*, derived from each term. Within the Mycenaean palaces the main ceremonial room, the so-called *megaron*, has been associated with the

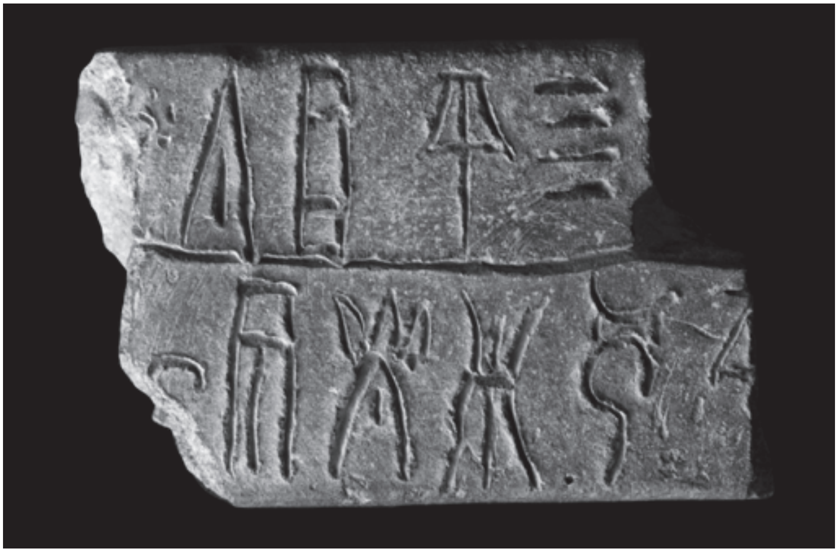


Figure 9
Linear B document (E 1569) found at Knossos recording plots of land measured in 'seed' grain; the second line lists a plot characterized by the epithet 'lawagesio-' (Ashmolean Museum, AN1938.710. Courtesy of the Ashmolean Museum, University of Oxford)

office of *wanax*. At Pylos and Tiryns, the existence of a second *megaron* has been linked in addition to the office of *lawagétas*. Like the *wanax* at Pylos, it is possible that the *lāwāgétās* may have appeared under his own name, if the identification with a major figure, *we-da-ne-u*, perhaps a priest of Poseidon, is correct.

Other titled members of the elite, attested at Pylos and Knossos, include the class called *hek^{w}etai* (Linear B *e-qe-ta*), perhaps 'followers (of the king)'. In the Pylos texts, *hek^{w}etai* appear not only with their names, but exceptionally also with a patronymic, emphasizing their aristocratic origins, and oversaw groups of military personnel in the much discussed An-series '*o-ka*' tablets, which appear to document forces deployed to watch Pylos' shoreline. As we have seen, cloth (at Knossos) could be characterized as 'for the *hek^{w}etai*' (Linear B *e-qe-si-jo/-ja*); the same is true of some chariot wheels at Pylos.

Although the above figures are often documented as 'acting' across the Pylian polity, they seem to have been centrally based. Other titled figures were associated with the sixteen or seventeen districts into which the Pylian polity was divided, as we saw above. The districts themselves may have been called *dāmoi* (Linear B *da-mo*), a term familiar in later Greek in a broad range of uses. The importance of the *dāmos* as an institution is implied by its appearance on a document (Un 718) with close parallels to the document mentioned above that lists the land holdings of the *wanax* and *lawagétas*. This parallel document contains offerings to Poseidon by Ekhelawon (not the *wanax*), the *lawagétas* and the *dāmos*. In another text about land holding (Ep 704, see pp. 28–9), the *dāmos* is a party to a dispute over the status of a plot contested by the priestess Eritha, implying its status as a legal entity, presumably distinct from the state, whose administrators recorded the dispute and may have been expected to settle it. It is possible that the *dāmos* controlled much of the land in the Pylos polity, since certain plots (of the type *ke-ke-me-na*) are said to be held 'from the *dāmos*'.

The official appointed by the king on the occasion of the compilation of the Ta tablets mentioned earlier was the *da-mo-ko-ro* and his name was Augewas. The first element of his title is probably *dāmo-*, implying his office oversaw the *dāmoi* for the palace centre; the second may be connected with the root of two other terms: *ko-re-te* and *po-ro-ko-re-te* (plural *ko-re-te-re* and *po-ro-ko-re-te-re*). These are clearly related and are often translated as 'mayor' and 'vice-mayor'. Each district had this pair of officials, as is shown by a document listing a polity-wide collection of bronze (Jn 829), where the *ko-re-te-re* and *po-ro-ko-re-te-re* each contribute an amount for all sixteen districts. These then appear to be officials with local or regional functions, but responsible to the central authority, where their activities were documented. Local terminology might have been more varied, however, since the tablet's heading refers to other titles, such as 'key bearer' or 'fig supervisor', implying their equivalence. The apparent oddity of such terms might be historical and we can think of similar status terms in British English, such as 'black rod'.

Despite the existence of titles for officials (even if they also appeared under their own names), it is clear that many members of the Mycenaean elite appeared in the documents simply under their own names. One such class has been termed by Linear B scholars 'collectors'. They are named individuals, possibly members of the royal family, who were assigned the benefit from (or perhaps owned) certain areas of production, such as stock rearing (at Pylos) or textile and oil production (at Knossos). Four have been identified at Pylos, including both *we-da-ne-u* and Alxoitas, whom we have already met, over twenty at Knossos, who also ran textile workshops in parallel to those centrally managed and were involved in the manufacture and possibly trade in perfumed oil. Parallel to the 'collectors' there existed a religious 'sector': certain animals and craftspeople are so characterized. Because both 'collector' and 'religious' stock and products were centrally recorded, it appears very likely that both were under the ultimate control of the central authority.

Mycenaean states in a broader context

As noted above, we neither have, nor can we reconstruct a 'constitution' for any Mycenaean state, even that of Pylos, for which the Linear B documents are most informative. The impression we have from the texts, however, is that the make-up of the institution we are accustomed to describe as a 'state' is less formal than application of that term implies.[14] Indeed, it is worth emphasizing that we have no idea how the 'Mycenaeans' at any site referred to themselves collectively, either in political or ethnic terms; usage of both the terms 'Mycenaean' and 'state' is ours, not theirs. It appears that an elite group – many based at Pylos, others at other locations within the polity – organized people and materials to support key productive activities. It is likely that the term *wanax* (and its associated epithet *wanaktero-*) represented an authority independent of any particular holder of that office, implying the existence of a 'state' or 'monarchy'. That authority appears to have been able, by means not explicitly stated in the texts, but no doubt involving, among other things, the 'carrots' of periodic banquets and the 'sticks' of military coercion, to command polity-wide contributions of bronze or the delivery of commodities as 'tax'. Whether the distinction between action in a titular role and action in name only represented a distinction between public (i.e. 'state') and private (as was common in many Near Eastern polities in the second millennium BC), or indeed, whether the distinction was recognized at all, lies beyond our current comprehension of the texts in their present state.

Our best route to understanding what *kind* of a world the Aegean was at the time of the Linear B tablets lies in comparison with more fully attested examples. Ventris and Chadwick made some specific comparisons with administrative systems in second-millennium BC Mesopotamia, such as those of Nuzi and Alalakh, while others, immediately following the decipherment, sought to compare the world of the documents with that embodied in the Greek texts closest in time to them, Homer's *Iliad* and *Odyssey*, largely to the latters' disadvantage. Cambridge historian Moses Finley most forcefully demonstrated to the scholarly world in a review of *Documents in Mycenaean Greek* how different the picture contained in the Linear B texts was from that in the Homeric texts, famously summing up the difference by stating that Homer 'was no guide at all' to the Mycenaean tablets of the Late Bronze Age.[15] Finley drew comparisons with the world of the Mesopotamian texts, particularly those of seventeenth-century BC Larsa in the Babylonian period, some centuries earlier than the Linear B texts. More important, however, than specific points of comparison, Finley argued that the overall system was similar: it was 'redistributive', with a single central authority – not markets – setting values and without evidence of equivalence, certainly without money in the modern sense.

Nicholas Postgate, another Cambridge scholar, has recently studied administrative practice comparatively across the Near East in the period 1400–1200 BC, from Assyria in the east to the Mycenaean polities in the west.[16] In general the proportion of administration carried out in writing declines the further west one travels and the administration of the small state of Ugarit shows similarities to those in the Mycenaean world, such as a tendency for writing to be confined to the centre and the use of a sealing system to manage transactions between the centre and those in outlying areas. Since we know from archaeological evidence that there were trade links between the Mycenaean world and Ugarit, it may be that aspects of administration were also appropriated along with trade goods, such as metals and ivory. Systems like that of the eastern *iškāru* might have inspired the Mycenaean *talasía* system, perhaps through links documented even earlier between Crete and the Levantine coast. Just as some see the eastern Mediterranean in the later Bronze Age as an interlinked world politically and culturally,[17] it may be that we should see it as linked in administrative practice too.

This idea of the Mycenaean palaces as single, totalizing central authorities has come under increasing scrutiny since Finley's day, and indeed the same is true for our scholarly understanding of the Mesopotamian palatial systems. We now view the Aegean systems as more pluralistic, more selective in their focus of monitoring and control, concentrated on certain key areas rather than on the total economy. Much went on in the overall economy without palatial involvement. These shifts in interpretation no longer depend on the decipherment of illegible texts; rather they are products of ongoing scholarly debate and the reformulation of ideas surrounding the structure and operation of these complex palace-centred systems. The raw data, however, that allow the sophistication of both our understanding and the terms of that debate we owe ultimately to the linguistically gifted young architect, Michael Ventris, whose modest and quiet voice announced the decipherment of the earliest European texts to a listening public in July 1952.

4

Other Pre-alphabetic Scripts of Crete and Cyprus

Philippa M. Steele*

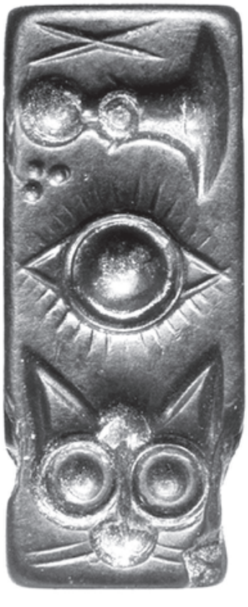
Linear B was only one of a series of related writing systems. It bears a close relationship with two earlier scripts in use in Crete during the Middle and Late Bronze Ages, and a more distant – but nevertheless very significant – relationship with the syllabic systems of Cyprus in the Late Bronze and Iron Ages. Most of these other scripts are considered to be undeciphered, with the exception of the Cypriot Syllabic script of the first millennium BC, which like Linear B was used to record the Greek language.

Cretan Hieroglyphic

Writing first appeared in Crete around the beginning of the Middle Bronze Age (about 2000–1800 BC) in the form of a system of quite pictorial-looking signs. Although the signs look like pictures of often recognizable entities like animals and body parts, they are not pictographic in the same sense as Egyptian hieroglyphs, where pictographic signs each represent whole words and can be combined to make sentences. In the Cretan writing system each sign represents a syllable, just as in Linear B. The only difference is that these signs look much more like small drawings of objects and animals than the later signs, which have become more linear and correspondingly more abstract. So the name 'Cretan Hieroglyphic' is really a misnomer that has remained in currency since the first categorization of Cretan writing systems made by Arthur Evans in his 1909 work *Scripta Minoa* (see chapter 1).

With only around 300 Cretan Hieroglyphic inscriptions surviving, our chances of deciphering the script and understanding whatever language is written in it are very small at present. Even so, a study of the inscriptions and the objects on which they are written can tell us a lot about the functions and context of writing. For example, a large proportion of surviving Cretan Hieroglyphic inscriptions are written on seal stones (figure 1). A larger number of clay documents bearing the impression

Figure 1
Seal stone made of green jasper and inscribed with a Cretan hieroglyphic inscription. The middle sign is easily recognized as a representation of an eye, and the bottom one as a representation of a cat's head
(Courtesy of Ingo Pini)



* The author would like to thank the European Research Council for funding the research mentioned in this article as part of the project Contexts of and Relations between Early Writing Systems; This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 677758).

of such seal stones has also been found, showing a connection between the inscriptions and administrative uses of writing. Cretan Hieroglyphic signs could also be written directly on to clay documents with a stylus, in a manner very similar to Linear A and Linear B.

The relationship between pictorial representation and writing is never more obvious than with Cretan Hieroglyphic,[1] and even though this script remains undeciphered it gives us some important clues about the origins of signs in other related writing systems. In Linear B it is still sometimes possible to identify what a sign was originally supposed to look like, especially when we are dealing with a sign that is used as both a *syllabogram* (representing a syllable like *a*, *ti* or *ko* and used to spell out words) and an *ideogram* (representing a whole concept or commodity, like *sheep*, *swords* or *cloth*). A good example is the syllabogram *mu* (moo!), which is also the ideogram for a cow, suggesting that the values of some syllabograms could be closely connected to what was represented by the corresponding ideogram. It is very common to find Linear B signs that have antecedents in Linear A (on which see below), but there are also some cases where we can identify a related sign in Cretan Hieroglyphic, like the cat's head sign shown in figure 1 (bottom sign), which in Linear A has become more abstract (often a triangle with two upper extensions for 'ears') but can sometimes be written in a more pictorial way (figure 2), while in Linear B it no longer looks very much like a cat at all. In Linear B we know that this sign stands for the syllable *ma* (𐀔), and it is very likely that it had the same value in the other scripts.

Even though we know less about it than we do about the other scripts, Cretan Hieroglyphic is a very important part of the story of writing in ancient Crete. It is furthermore striking that Cretan Hieroglyphic signs appear to be new creations, with little evidence to corroborate a long-standing view that the script was based on, or created with knowledge of, other writing systems around the Mediterranean such as Egyptian hieroglyphs. In turn this suggests that the earliest development of writing in Crete was an innovative and transformative process, and one that was to have long-lasting effects on the island.

Linear A

Appearing shortly after Cretan Hieroglyphic, and co-existing with it for perhaps two or three hundred years, was another writing system that we

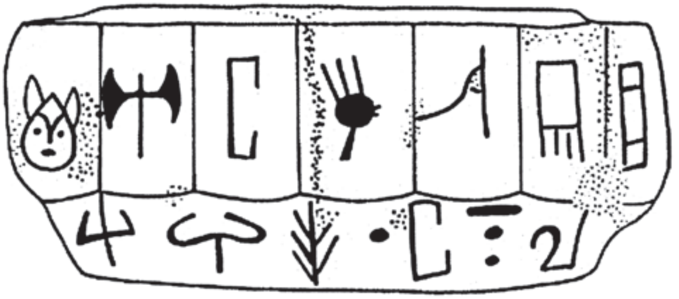


Figure 2
Line drawing of one side of a Linear A inscribed stone vessel. The first sign on the top left is an elaborate version of the cat's head sign. (After Godart and Olivier 1976–85, vol. 4, IO Za 2)

call Linear A. Again we owe the term to Arthur Evans's categorization of Cretan writing, who saw this system as more linear-looking than Cretan Hieroglyphic – and, again, the term remains in currency today, over a hundred years after it was coined. Based on our modern impression of the distinctive features of each script, it is usually possible to classify any given inscription as being written in either Cretan Hieroglyphic or Linear A. However, we do not understand very well why the two scripts co-existed with each other for so long, or to what extent their users viewed them as separate entities.

Linear A remained in use for longer than Cretan Hieroglyphic, lasting into the second phase of the Late Bronze Age (around the fifteenth century BC), by which time it was written almost exclusively on clay documents like tablets and sealings. However, over the several hundred years when it was in use, we have a clear indication that Linear A was not restricted to clay administrative documents alone because a small number of other inscribed items have survived. These include items of jewellery made of silver and gold, such as pins and rings, as well as bronze axe heads, pottery vessels and stone vessels. The last of these categories, usually consisting of slabs of stone with a hollowed-out basin, are particularly intriguing because their inscriptions often include elements of a repeated formula, possibly related to a religious use for the items. Overall, however, it is the clay tablets and sealings that make up the overwhelming majority of the surviving corpus of inscriptions, with around 1,500 examples.

Linear A is clearly much more closely related to Linear B than is the Cretan Hieroglyphic script. We can observe very close affinities in the shape of Linear A and Linear B signs, to the extent that it is possible to identify more than 70 per cent of Linear B signs with Linear A antecedents. There are also very good reasons to believe that Linear B did not make drastic changes to the values of most signs, which means that we can use the deciphered Linear B script to 'read' Linear A.[2] In practice, however, this does not mean that we understand the language of Linear A: surviving Linear A inscriptions do not contain vocabulary items that can confidently be identified as belonging to any other known language. By contrast, the successful decipherment of Linear B was owed in part to its superior numbers of surviving inscriptions (four times as many as we have for Linear A) and in part to the fortunate coincidence that the language recorded in it was a well understood and recognizable one, namely Greek. Whatever the language of Linear A, which is often referred to as 'Minoan', we can be sure at least that it is not Greek.

In the current state of knowledge, it seems unlikely that the language written in Linear A could be fully understood without further discoveries of long inscriptions that could give us some clues to its identity. Nevertheless, a study of the inscriptions we have can be very fruitful. Sometimes place names or personal names that are attested in Linear B documents also appear in Linear A documents, such as the place name Phaistos (*pa-i-to*) in southern Crete – the name is still in use today. Looking at patterns in Linear A sign sequences also allows a study of some of the language's morphological properties, which look quite different from those of Greek. Occasionally we can even work out the meaning of a word. The best example is the word *ku-ro*, which appears at the end of lists of commodities: the numeral that follows *ku-ro* is the sum of each of the individual numerals in the list entries, and so we can identify the word *ku-ro* as meaning 'total'.

Many of the individual words in surviving Linear A inscriptions occur only once, or recur only infrequently, which again makes it difficult to try to ascertain what sort of word we are dealing with in any given case – for example, whether a word is a noun, a person's name, a verb, etc. The best opportunity to try to understand the construction of a sentence is found in the so-called 'libation formula': a recurring set of words that often appear on stone vessels with hollows, whose purpose is thought to be religious. Variants of several words reappear together in this context: *a-ta-i-*301-wa-ja*, *a-di-ki-te* (which could be related to the name of Mount Dikte, also found in the Linear B tablets), *ja-sa-sa-ra-me*, *u-na-ka-na-si*, *i-pi-na-ma*, *si-ru-te*. However, the exact composition of the 'phrase' as well as the exact form of each word can vary from one inscription to another, making it more challenging to try to reconstruct how the words fit together. The more evidence we have, the better our chances of making sense of such inscriptions, and further advances are entirely possible following the sorts of careful methods that were employed in the decipherment of Linear B.

The story of how Greek speakers came to adopt the Linear A script and create the one that we call Linear B is not very easy to reconstruct. Once envisaged as a violent episode in which Mycenaeans ousted Minoans from their native land, we now better understand this period as one of gradual if decisive transition. Where previously there had been regional administrative centres in different areas of the island, in the period between 1450 and 1375/1350 BC it looks as though power was concentrated at Knossos in the north of Crete. This may be where Greek speakers encountered the use of Linear A in administrative documentation, and adapted it for their own uses; at quite an early stage the new Linear B script was transferred to Mycenaean centres in mainland Greece along with the administrative processes with which it was associated. What is striking is that although the Mycenaean Greek speakers made some changes, their methods of bureaucratic administration were very much modelled on those of their Minoan predecessors, in particular the types of documents in which Linear A records had been kept.

Mycenaean Greek speakers seem however to have had a different attitude to writing and what it could be used for. Linear B was restricted almost completely to bureaucratic clay documents, and even the few exceptions to this rule (for example, a number of stirrup jars with painted inscriptions) seem to belong to the administrative sphere. The more 'private' uses of writing witnessed in Linear A, such as inscriptions on pieces of jewellery and votive items, were apparently abandoned.

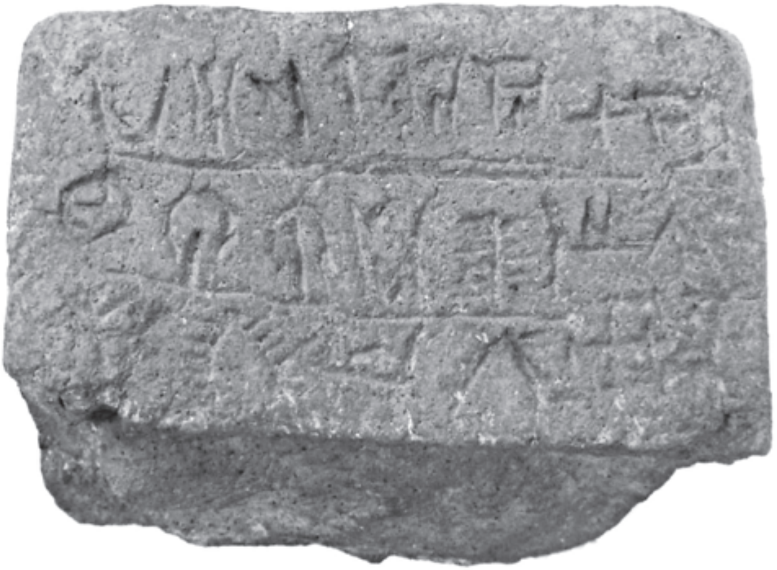


Figure 3
One of the earliest Cypro-Minoan inscriptions, written on a clay tablet. (Courtesy of Silvia Ferrara)

Cypro-Minoan

Linear B was not the only writing system to be derived from Linear A. At some point around the beginning of the Cypriot Late Bronze Age (the sixteenth or early fifteenth century BC), a new system based on Linear A was adopted in Cyprus. This adaptation created a quite different-looking system that is usually labelled Cypro-Minoan, again based on Arthur Evans' categorisation. Although one of the earliest surviving texts, a clay tablet from Cyprus, has quite a Linear A 'look' to it (figure 3), most of the 250 surviving Cypro-Minoan inscriptions are somewhat different in appearance. This means that it is not a simple task to try to work out how each of its signs might be related to Cretan predecessors in Linear A.

Despite the smaller number of surviving inscriptions in Cypro-Minoan (which has the smallest corpus of all the Aegean scripts), we have enough to be able to identify some signs that are very clearly related to ones in Linear A. Even better, we can reconstruct the values of the signs using the values of signs in a later Cypriot script derived from Cypro-Minoan, usually called the Cypriot Syllabary and used often to write the Greek language (see the next section). It is very striking that there are about ten or eleven signs that have the same values in the Cypriot Syllabary and in Linear B (both scripts used for Greek, which means we can understand them). If they share the same values in these two scripts, this must be because they also had the same value in the ancestor of each script, i.e. Linear A (the script from which Linear B was derived) and Cypro-Minoan (the script from which the Cypriot Syllabary was derived). So, we can for example reconstruct the value *ti* for an arrow-shaped sign found in all four of these scripts (figure 4 overleaf), and the same can be said confidently for a handful of other signs.

Although it is probably the case that the shapes and perhaps even values of a number of signs changed in the adaptation of Cypro-Minoan

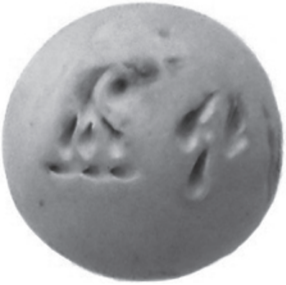


Figure 4
Clay ball with a Cypro-Minoan inscription; the sign on the right is the arrow-shaped sign, 'ti'. (Courtesy of Silvia Ferrara, with digital enhancement by Philip Boyes)

from Linear A, the core of ten or eleven signs whose values can easily be reconstructed proves the close relationship between these writing systems. For the other signs, a study of developments in their shape over time can help us to try to understand where each sign came from and what it developed into.[3] Such palaeographical analysis has the potential to reveal links between the signs that are not always obvious when looking at any single inscription, and it is very important to consider the whole range of inscriptions, as well as the effect of using a different medium: for example, it is possible to achieve more rounded shapes when incising in wet clay than it is when incising on a surface like hard metal or stone.

Although there are clearly some advances that can be made in the study of Cypro-Minoan, it has not yet been possible to understand the language (or perhaps languages) written in it. One reason is the small number of inscriptions, as well as their short length (the vast majority of the surviving 250 inscriptions are ten signs long at a maximum, and most are shorter than that), which means that we have very little material to analyse. Another problem in this regard is the diversity of the inscriptions. Cypro-Minoan is attested between the sixteenth/fifteenth century to the tenth century BC, and over the five hundred years or more when it was in use, it was written on a wide variety of different objects.

Like the other Aegean scripts, Cypro-Minoan is sometimes found on clay tablets and other documents like labels and cylinders. The most popular surviving clay document type is, however, of a type not found in Crete, namely the clay ball: these were small spherical pieces of clay with short inscriptions running around the outside (figure 4), a very distinctive Cypriot object with few parallels elsewhere. There were also numerous other types of objects bearing inscriptions, including items of jewellery, bowls made of silver and bronze, votive items including clay figurines and ivory pipes, bronze 'spits' and miniature ingots, stone and especially clay vessels of various sizes and shapes. This array of inscribed items tells us something very important about Cypriot literacy in the Late Bronze Age, namely that writing was perceived as suitable for use in many different spheres of life. This might remind us of the situation found in Linear A, while it stands in stark contrast with the situation in Linear B.

While Cypro-Minoan may not be easy to decipher, given the small amount of inscribed material surviving, there is in fact great potential for understanding the context of Cypriot writing in the Late Bronze Age.

Studying the range of inscribed objects and their archaeological context can tell us a great deal about the role of writing in society.[4] Meanwhile, the position of Cypro-Minoan as 'daughter' of Linear A, 'sister' of Linear B and 'mother' of the Cypriot Syllabary – to envisage the relationships as a family tree – gives us some significant advantages in an attempt to reconstruct the values of Cypro-Minoan signs. With further finds of inscriptions coming to light every so often in archaeological excavations, better understanding of the content of inscriptions may one day be tantalisingly within reach.

The Cypriot Syllabary

The last of the Aegean writing systems is the also the latest, the Cypriot Syllabary, a system developed from Cypro-Minoan and used in Cyprus for hundreds of years from at least the eighth century to the third or second century BC. It was used to write Cypriot Greek during this period, and also to write a local Cypriot language that we do not understand, known today as 'Eteocypriot'. As a syllabic system broadly similar in appearance to the other Aegean systems, the Cypriot Syllabary occupied the odd position of being the only non-alphabetic script used for Greek anywhere in the Mediterranean at this time. Elsewhere, it was the very prolific Greek alphabet that was used, developed from the Phoenician alphabet and passed on to other areas including most significantly Italy, where Etruscan and Latin speakers also adopted it. The continued use of the Cypriot Syllabary to write Greek in Cyprus throughout this period looks very much like a statement of Cypriot identity and independence.

The Cypriot Syllabary was in fact the first of the Aegean scripts to be deciphered. The decipherment was made long before that of Linear B, by the Assyriologist George Smith in the nineteenth century. The basis for his decipherment was a bilingual inscription with parallel texts written one above the other in Phoenician and Cypriot Syllabic Greek, discovered at the site of Idalion in central Cyprus (figure 5 overleaf). Phoenician, an alphabet in which only consonants were represented, had already been deciphered and so could be understood reasonably well, thus providing the sense of the text. Most words and phrases in the bilingual had to be translated to understood, but there were some names that had close parallels in both the Phoenician and the Cypriot Greek halves of the text. In the top line, for example, the Phoenician phrase *MLK MLKYTN*, 'of King Milkyaton', is paralleled in the first line of the Cypriot Greek half, where the phrase *pa-si-le-wo-se mi-li-ki-ya-to-se* has the same meaning (*mlk* and *basileus* being respectively the Phoenician and Greek word for 'king'), and the name Milkyaton is spelt in a similar way in both halves. Working through the whole inscription therefore gave important clues to the values of Cypriot Syllabic signs.

The decipherment of the Cypriot Syllabary was achieved by Smith, and aided by the work of other nineteenth-century scholars such as Moritz Schmidt, Wilhelm Deecke and Johannes Brandis. It was this great step forward in our understanding of one of the Aegean scripts that

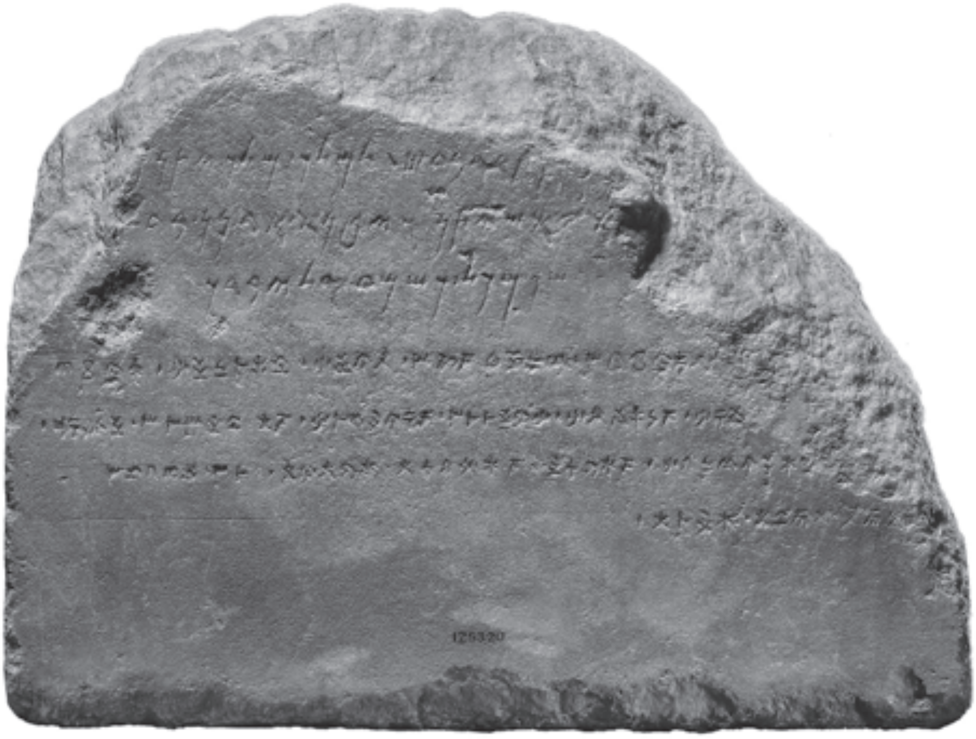


Figure 5
Bilingual inscription in Phoenician (at the top) and Cypriot Syllabic Greek (below). (British Museum 125320, © Trustees of the British Museum)

unlocked the potential to decipher others. The stability of the shape and value of some signs across the Aegean scripts meant that when scholars in the twentieth century began to attempt decipherment of Linear B, they could already be confident of the values of some of its signs. Nevertheless, the task was not straightforward: the signs of the Cypriot Syllabary had undergone a number of developments since the original adaptation of Cypro-Minoan from Linear A, leaving only about ten or eleven that were close enough in shape and value to allow certainty in reconstructing them. The values of other signs of Linear B had to be reconstructed via a much more complex process (see chapter 2).

Even though it is formally 'deciphered', there still remain a few unanswered questions surrounding the use of the Cypriot Syllabary. One of the most intriguing is the use of this script to write an otherwise unknown language that has been labelled by modern scholars as 'Eteocypriot'. Only about twenty-five Eteocypriot inscriptions survive, and although we can reconstruct some features of the language (for example a probable case system and some of its phonology), the content of most of the inscriptions remains mysterious.[5] Even the survival of one complete and three fragmentary bilingual inscriptions (in Eteocypriot and Greek) has not helped very much, perhaps because the Eteocypriot language is not closely related to any well-understood languages known today.

The Cypriot Syllabic script persisted throughout the age of the city kingdoms in Cyprus, when the island was divided between independent cities with their own kings, who sometimes used Cypriot Syllabic inscriptions to mark events of their reign and on their coinage. During this period, the script enjoyed quite widespread use: not only were there 'public' inscriptions issued by royal dynasties and found in religious sanctuaries, but there have also survived numerous inscriptions of a more 'private' nature, including gravestones and graffiti on pieces of pottery. In the fourth century BC, mercenaries serving in the armies of Egyptian pharaohs were literate enough to write their own names on the walls of Egyptian temples, and there is even a Cypriot Syllabic graffito on a block of the Great Pyramid of Khufu. At the end of the fourth century BC however, Cyprus became politically unified under the Ptolemaic dynasty, at which point the Greek alphabet was adopted as the writing system used for official inscriptions. The surviving epigraphic record suggests that the Cypriot Syllabary went out of use within the next one or two centuries, putting an end to the last of the Aegean scripts.

Future directions

There remain enough mysteries surrounding the Aegean scripts and their relationships with each other that scholars today are still researching and shedding new light on these issues all the time.[6] In some cases, we may be able to make progress towards decipherment, but decipherment is not the only goal of such studies: analysing the surviving inscriptions of Crete, Greece and Cyprus in the Bronze and Iron Ages has great potential for helping us to understand literacy and the role of writing in society, as well as the relationships between different groups of people who passed writing on from one to another.

A new research project based in Cambridge, *Contexts of and Relations between Early Writing Systems*, has recently begun to explore such relationships between the Aegean scripts in comparison with the development of early alphabetic scripts of Greece and the Levant, showing the potential for the study of broader connections that can help us to understand why and how writing systems change. Meanwhile, new inscriptions can often come to light in ongoing archaeological excavations, and with every new inscription comes the hope of a better understanding of the languages and writing systems of the ancient Aegean and Cyprus.

5

Aegean Scripts in a Digital Era

Federico Aurora

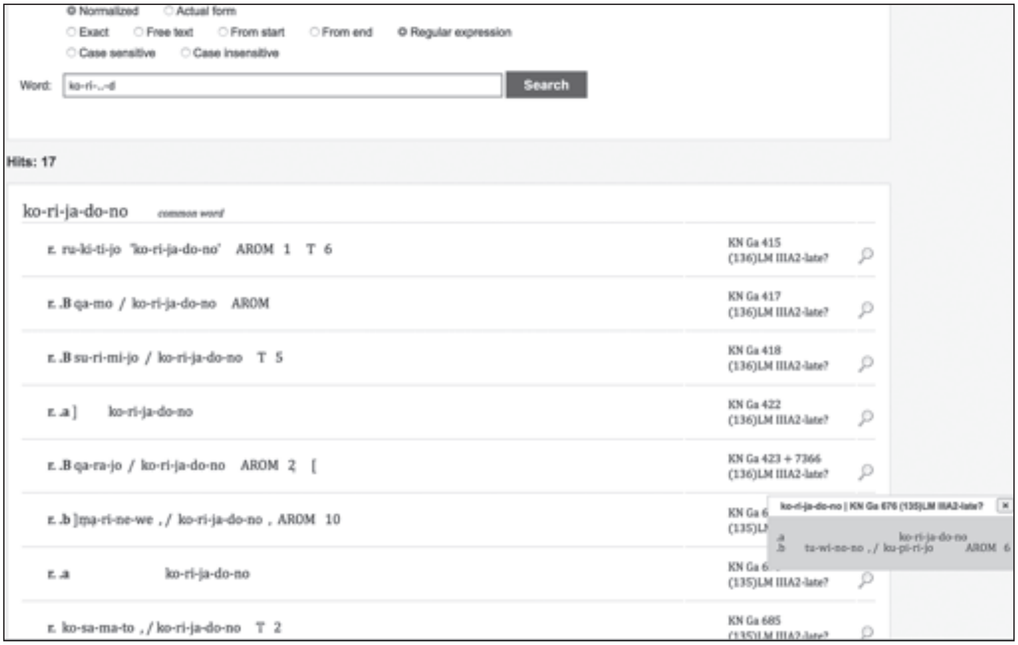
Classics was among the first fields within the humanities to use computing tools and methods. The pioneering work of Roberto Busa, who as early as the 1950s started working on machine-generated concordances of the Latin text of the *Summa Theologica* of Thomas Aquinas, is often mentioned as the starting point not only of computational linguistics but of 'Digital Humanities' as a whole. The last two decades have seen a profusion of digital resources for the study of the ancient world: from three-dimensional digital reconstructions of ancient sites to text databases containing most of the surviving Greek and Latin literature, from dictionaries and study tools to comprehensive databases of non-literary documents such as inscriptions, papyri and wooden tablets. An overview of this wealth of available resources, which are mostly open access, can be gleaned from the Digital Classicist wiki.[1]

Mycenological and Aegean studies are no exception to this general trend. John Younger, then at Duke University and now in the University of Kansas, started as early as 1993 what is still the main mailing list for Aegean subjects, Aegeanet,[2] and published his web pages with Linear A texts as early as 2000. A lot more resources have appeared in the last decade.

If the combination of the study of antiquity and the use of modern computing tools and methods might be at first surprising, on closer inspection it will appear to be a quite natural consequence of the subject matter of classics. This is the study of past worlds, quite remote from ours, through their literature and physical remains which have reached us in fragmentary state, and need to be reconstructed and somehow recreated. Computing and digital resources evidently offer new possibilities for this reconstruction enterprise. In addition to providing scholars and students with powerful tools and resources, this digital turn in classics has also yielded a much better access to antiquity for the general public, also thanks to the open access – and therefore free of charge – policies fostered by the digital means of publication and embraced by many classics projects.

Resources on the Linear B script

The first online publication of a large searchable database of Mycenaean texts occurred in 2011 on the website Deaditerranean.[3] This website,



● Normalized ○ Actual form
○ Exact ○ Free text ○ From start ○ From end ● Regular expression
○ Case sensitive ○ Case insensitive

Word: ko-ri-..-d

Hits: 17

ko-ri-ja-do-no *common word*

r. ru-ki-ti-jo 'ko-ri-ja-do-no' AROM 1 T 6 — KN Ga 415 (136)LM IIIA2-late?

r. .B qa-mo / ko-ri-ja-do-no AROM — KN Ga 417 (136)LM IIIA2-late?

r. .B su-ri-mi-jo / ko-ri-ja-do-no T 5 — KN Ga 418 (136)LM IIIA2-late?

r. .a] ko-ri-ja-do-no — KN Ga 422 (136)LM IIIA2-late?

r. .B qa-ra-jo / ko-ri-ja-do-no AROM 2 [— KN Ga 423 + 7366 (136)LM IIIA2-late?

r. .b]ma-ri-ne-we ,/ ko-ri-ja-do-no , AROM 10 — KN Ga 6 (135)L

ko-ri-ja-do-no | KN Ga 676 (135)LM IIIA2-late?
.a ko-ri-ja-do-no
.b tu-wi-no-no ,/ ku-pi-ri-jo AROM 6

r. .a ko-ri-ja-do-no — KN Ga 6 (135)LM IIIA2-late?

r. ko-sa-ma-to ,/ ko-ri-ja-do-no T 2 — KN Ga 685 (135)LM IIIA2-late?

Figure 1
A search in DĀMOS for texts where ko-ri-ja-do-no ('coriander') is mentioned (Courtesy of DĀMOS, University of Oslo)

the produce of Kim Raymoure, an independent scholar, is the best of several amateur scholars' web pages on Aegean philology that one can encounter on an Internet stroll. Deaditerranean provides most of the texts in transliteration, although not always updated according to their last edition and without their original layout on the Linear B tablet. The site also provides an index of scribal hands and a very concise dictionary of most logograms and words. All the information given is documented with bibliographical references, albeit often rather outdated.

Regularly updated texts according to the most recent scholarly publications can be found in *DĀMOS: Database of Mycenaean at Oslo*,[4] a resource created by the author in 2013, and *LiBER: Linear B Electronic Resources*,[5] a project of Maurizio Del Freo and Francesco Di Filippo of the Institute for the Study on Ancient Mediterranean (also available since 2013). The former project contains all the published Linear B documents in transliteration. The latter project, at the moment, contains the transliterated texts from Mycenae, Midea and Tiryns. Both databases allow browsing through the texts or a given subgroup, which the user can define by filtering the records through an ample set of metadata. So one can, for example, choose to look for all Knossian documents attributed to hand 135 belonging to the 'Ga series', where scholars have grouped tablets registering different kinds of spices, and obtain a subgroup of 15 tablets. The Fitzwilliam Museum tablet, KN Ga 676, belongs to this group (for further discussion see chapters 2 and 3). Within a given subgroup, or the whole corpus, one can further perform word searches, in order, for instance, to discover which other tablets in addition to Ga 676 record coriander quantities (figure 1).

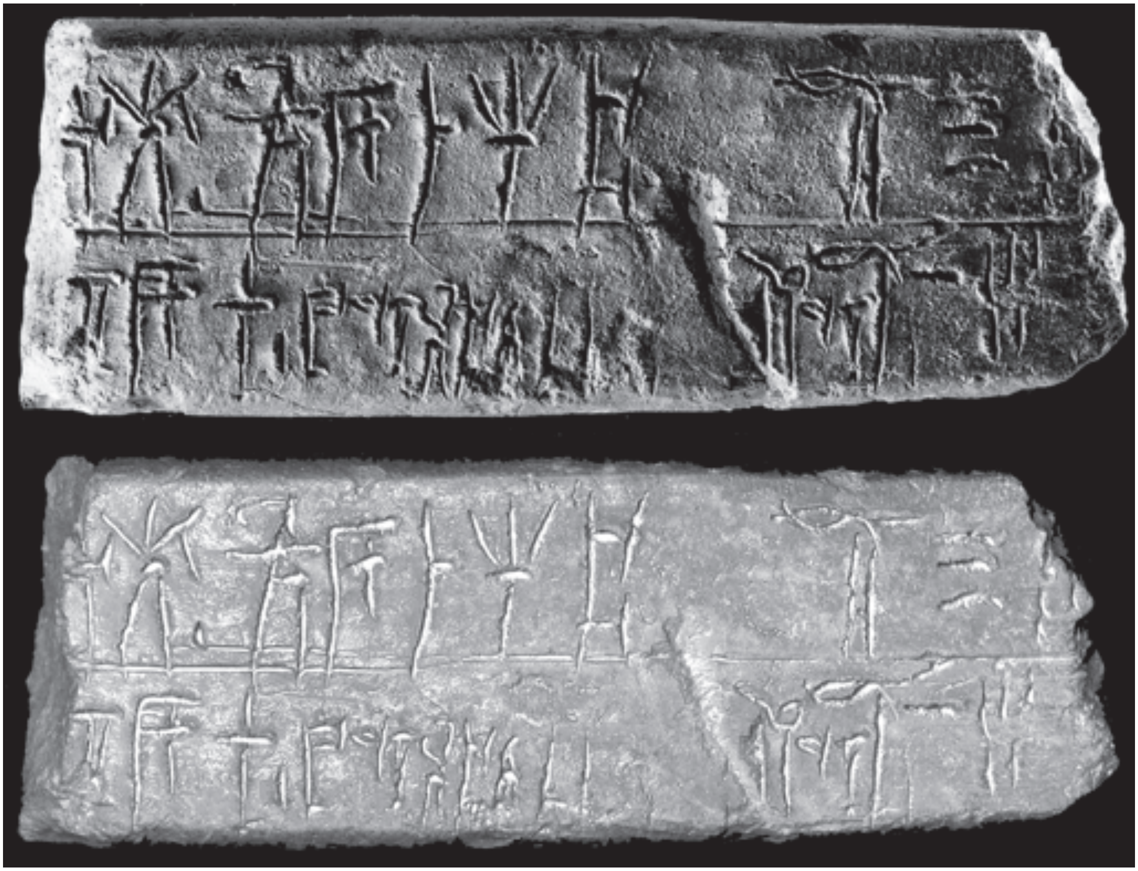


Figure 2
Two visualizations in RTIViewer with different light features of one of the digitised tablets from Knossos (KN Dl 47) (Ashmolean Museum, AN1938.709. Courtesy of the Ashmolean Museum, University of Oxford)

In addition to text databases, scholars now have access to images of Linear B documents. Until recently, only a few images were available on the internet, but the situation has dramatically improved in the last five years. In 2012 Yannis Galanakis, then curator of the Aegean collections at the Ashmolean Museum in the University of Oxford, published online the pictures of the museum's small but representative collection of Linear B tablets from Knossos on the occasion of the sixtieth anniversary of the decipherment.[6] Galanakis was inspired by the work of the *Cuneiform Digital Library Initiative* project – an international digital library project that aims to record text and images of around 500,000 cuneiform documents. He liaised with the Oxford team of Jacob Dahl, Klaus Wagensonner and Nicholas Reid, who were at the time digitizing cuneiform tablets using the Reflectance Transformation Imaging technology. This technology results in a faithful interactive image of the artefact, which, when opened in a specific viewer (RTIViewer)[7] allows the user to inspect the object under varying illumination angles and other features of light, such as colour or intensity. This technology therefore allows scholars to examine documents literally under a completely different light. Considering the fact that Mycenaean tablets do not photograph well with traditional cameras, this

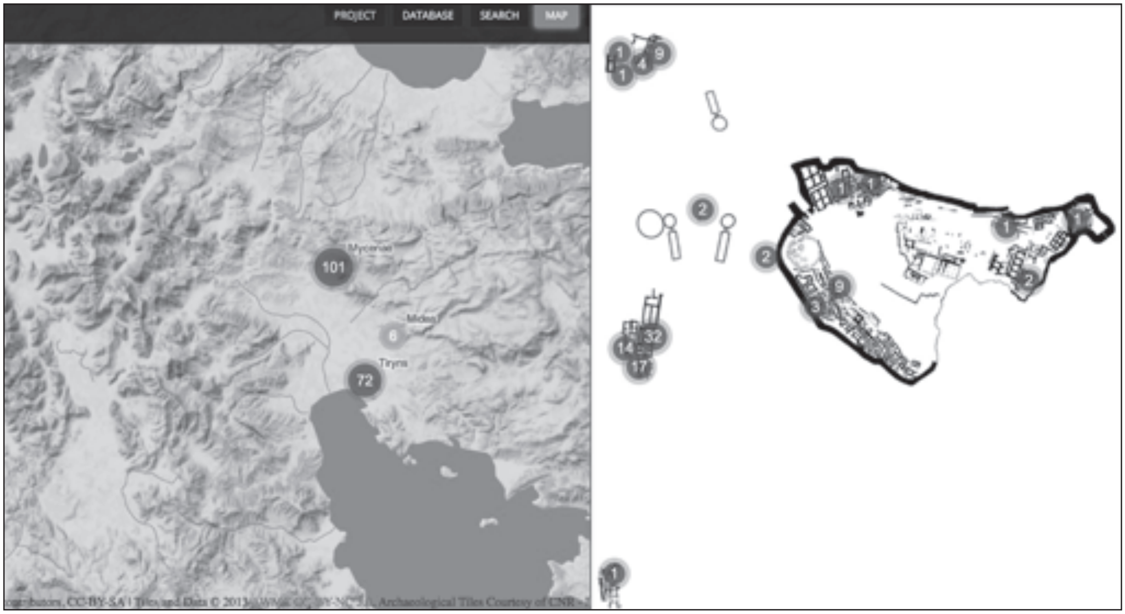

PROJECT
DATABASE
SEARCH
MAP
Mycenae
101
Midea
6
Tiryns
72
contributors, CC-BY-SA | Tiles and Data © 2013 AWMC CC-BY-NC 3.0 | Archaeological Tiles Courtesy of CNR
1
4
9
2
32
14
17

Figure 3
Images from two different zoom levels of the map contained in LiBER, showing respectively the number of documents per site (higher scale level) and the number of documents per find-spot in Mycenae (lower scale level)
(Courtesy of the Institute for the Study on Ancient Mediterranean)

imaging approach, first used by the Ashmolean Museum for Linear B documents, provides a much better access to them, both for scholars and the general public (figure 2).

With this aim, the Pylos Tablets Digital Project, led by Dimitri Nakassis of the University of Colorado Boulder, and Kevin Pluta, of the University of Texas at Austin, is combining the traditional methods for documenting the tablets (transcriptions and drawings) with RTI and three-dimensional scanning, for the forthcoming new edition of the Pylos Linear B tablets. To date, however, the only comprehensive collection of images of the Pylos documents is the repository of the University of Cambridge Linear B Research Archive (CaLiBRA),[8] maintained by the Mycenaean Epigraphy group in the Faculty of Classics, which in 2015 took the initiative to digitize the black-and-white pictures taken in 1963 at the University of Cincinnati.

As to the other sites, LiBER provides black-and-white pictures of the tablets from Mycenae, Tiryns and Midea, while pictures of almost all Mycenaean seals, some nodules with seal impression and a few tablets, are available through Arachne, the central object database of the German Archaeological Institute (DAI).[9] Finally, black-and-white pictures of a selection of Linear B documents from Knossos are contained in Evans' *Scripta Minoa* (vol. II, 1952), digitized in 2007.[10]

In addition to texts and images, LiBER also provides maps of the sites of Mycenae, Tiryns and Midea, where the data obtained by database queries can also be plotted. The maps are georeferenced, that is they have been mapped onto the international system of geographic co-ordinates and can thus be shown in their real position on a world map (figure 3). Since 2011 we have online the indexes to Francisco Aura Jorro's *Diccionario Micénico*, the standard reference dictionary for Linear B, in Spanish. A new edition of the dictionary is also scheduled to be published online. It will represent a milestone for the digital development of Mycenaean studies.[11] At the moment, though, the only (partial) dictionaries available online are the short Mycenaean–English dictionaries at the amateur websites Palaeolexicon,[12] which also includes dictionaries of Cypriot Syllabic script and Eteocypriot, Deaditerranean and the Mycenaean Wiktionary.

As for the other pre-alphabetic writing systems in the Aegean, the Linear A texts, as previously mentioned, were the first to appear online.[13] They are published in a normalized form that is, transliterated according to Linear B phonetic values and given a standardized format. In the same online resource, and since 2005, one can also find normalized transcriptions of Cretan Hieroglyphic texts and pictures, and transcriptions of the Arkalokhori Axe and of the infamous Phaistos Disc. The site provides also lexica, bibliographies and a thorough introduction to the scripts. Recently PDF versions of the standard editions of these corpora have been made available online,[14] while older black-and-white pictures can be found in Evans's *Scripta Minoa* volume 1 (1909), digitized in 2007.[15]

Computational tools for linguistic analysis – and new decipherments?

In addition to all the texts of the Linear B corpus, DĀMOS also contains their linguistic annotation, that is linguistic information (morphological, syntactical and semantic) about each text, sentence and word. This allows for quantitative investigations of the language of the tablets and the application of statistical methods to its study.[16]

What about the use of computational tools then for deciphering the still undeciphered scripts? In 2010 a paper entitled 'A Statistical Model for Lost Language Decipherment' was published in which the authors proposed a method for the automatic decipherment of undeciphered languages with the help of a corpus of a known, possibly related, language. The idea was to computationally 'encode some of the linguistic intuitions that have guided human decipherers'.[17] As a test of the method, they presented their successful redecipherment of Ugaritic, a Semitic language related to Hebrew, first deciphered in 1930. Following this line, in 2016 Richard Sproat and Kyle Gorman of Google Research began the redecipherment of Linear B with ancient Greek as parallel corpus. The work has just started, but the undertaking is a very exciting one. Especially if one thinks of the possibilities these methods could open for the still undeciphered Aegean scripts – even though it is worth remembering that the current scholarly consensus is that we have too little material to decipher even Linear A let alone the Cretan Hieroglyphic script. Nonetheless, for just this purpose, a digital corpus of Linear A, still unpublished, was created in 2014 by a team led by Francesco Patrono Cacciafoco of Nanyang Technical University in Singapore, in order to try to apply computational methods to the deciphering enterprise. As of 2017 their work is still in progress.

Other online resources

A brief overview of the Aegean scripts is given by the *Oxford Classical Dictionary* online[18] and a more detailed one in the *New Pauly* online,[19] but the best overviews available in the internet are those contained in the *Encyclopaedia of Ancient Greek Language and Linguistics*.[20] None of these three resources, however, is open access. The best open access scholarly overview of the Aegean scripts is probably the one at *Mnamon*, the portal about ancient writing systems of the Mediterranean of the Scuola Normale Superiore of Pisa.[21]

Wikipedia's English pages on the Aegean scripts seem to be of a good standard. It is also interesting that a good number of Wikipedia's articles on Aegean or Ancient Greek subjects have links to the original texts (e.g. DĀMOS or Deaditerranean), providing a low-threshold point of access to the content of the Mycenaean documents. For the history of the discovery of the Aegean scripts and of the decipherment of Linear B, mention needs to be made of two important recent digitization projects: of the Sir Arthur Evans archives, regarding his Knossos excavations, at the Ashmolean Museum,[22] and of the digitization of the archives of Michael Ventris[23], Alice Kober[24] and Emmett L. Bennett Junior by the Program in Aegean Scripts and Prehistory (PASP) of the University of Texas.[25]

Fonts, freely downloadable, based on a standardized version of the signs have been created for all the Aegean scripts except Cypro-Minoan. These, while not irrelevant for researchers, are very useful for didactic and dissemination purposes. A detailed overview can be found in *Mnamon*.[26] Other useful portals for Aegean matters are the web pages of the Mycenaean Epigraphy group at Cambridge,[27] and of Aegeus, the Society for Aegean Prehistory.[28] Nestor, a regularly updated bibliography on Aegean matters of the University of Cincinnati, is also an excellent starting point for all those interested in finding more literature on the subject.[29]

Connecting resources

An important task for the future, besides creating new resources and developing the existing ones, is to organically connect them with each other and, then, to relevant archaeological material, to be found in databases like the already mentioned Arachne or those accessible through the Aegean Museum project (University of Florence).[30] This would then bring together data from different sources and produce a virtual representation, as complete and integrated as possible, of the world of the Aegean scripts. Teamwork, a defining element of the decipherment of Linear B and of Mycenaean studies in general, is also a crucial element for connecting resources, across platforms, in a sustainable and dynamic way paving the future of Aegean scripts in a digital era.

6

Classics at Bletchley

Annie Burman

Since the declassification of the codebreaking efforts of the Second World War, the story of Bletchley Park has become well known. Originally confined to seventy people in the eponymous Victorian manor house located half way between Oxford and Cambridge, British cryptanalysis encompassed many thousands of people by the end of the war. The most famous is without a doubt the mathematician and computer scientist Alan Turing (see chapter 8). Many other prominent codebreakers from the Second World War shared his scientific background. For example, Gordon Welchman (1906–85), who together with Turing developed the Bombe, a machine that sped up the breaking of German codes, was a fellow of mathematics at Sidney Sussex College in Cambridge, while Irving Jack Good (1916–2009) studied mathematics at Jesus College, also in Cambridge, and worked with statistics and computing after the war.

Yet not everyone at Bletchley Park was a mathematician. In the early days of the Government Code and Cipher School (GC&CS), as the forerunner of the modern Government Communications Headquarters (GCHQ) was called, many of the highly educated members came from an altogether different background. The roots of this practice should be traced back to the First World War. No organization comparable to GC&CS existed at the time. Instead codes were handled separately by the army, in section M11b, and the navy, by a small group referred to as Room 40 after their headquarters in the Admiralty.[1] The encoded intercepts they handled were also quite different. All were manual codes, encrypted with the help of codebooks.

It was into this context that the most famous classicist at Bletchley Park first entered the world of cryptanalysis. Dillwyn Knox (1884–1943) studied classics at King's College in Cambridge, eventually becoming a fellow (figure 1). When the First World War broke out, he was working on a critical edition of the *Mimes* of Herodas – short humorous dramatic scenes in verse – which had only survived on a badly damaged papyrus (published 1922). In 1915 he put his work in classics aside and joined Room 40. Like him, many of the cryptanalysts there were classicists. The codes were approached as unknown languages and cracked with diligence and persistence.

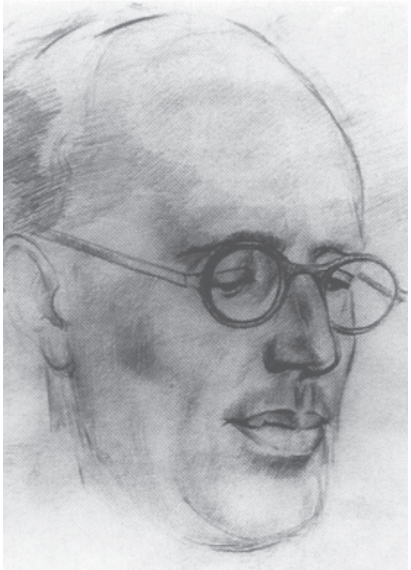
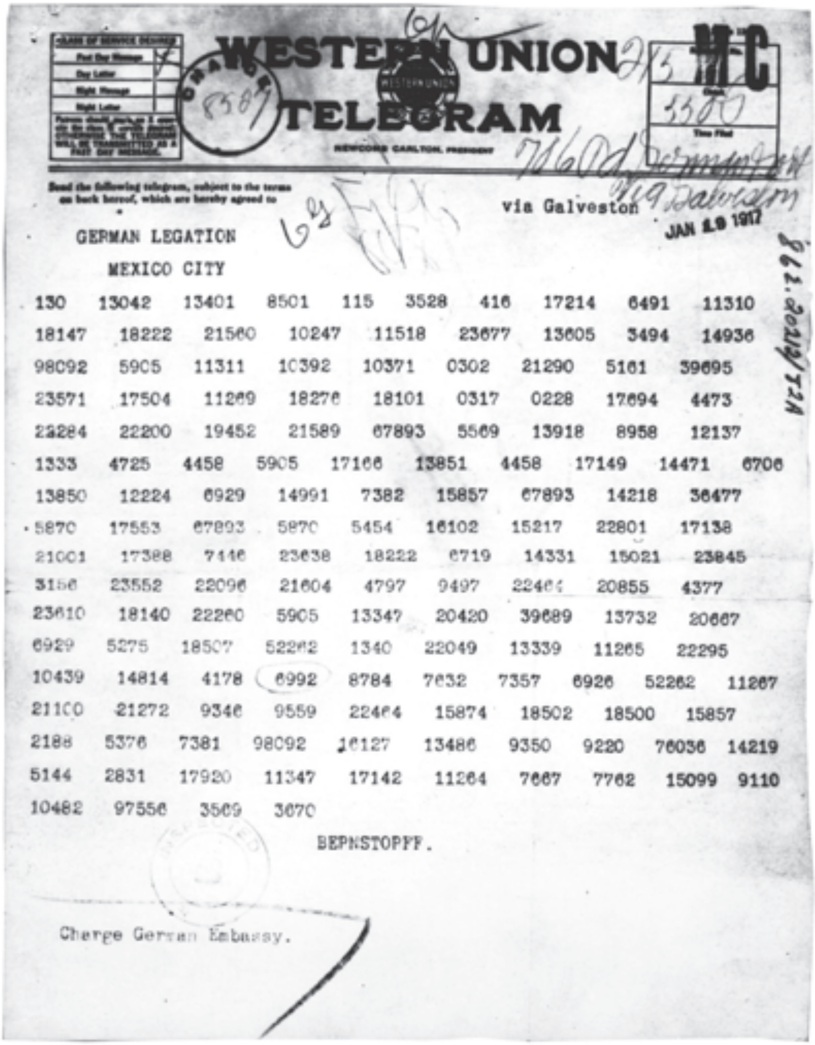


Figure 1
Dillwyn Knox captured in thought
(By kind permission of the Government's Communication Headquarters)

In 1917 the United States entered the war, partly as a result of a telegram from the German Foreign Secretary Arthur Zimmerman that proposed an alliance between Germany and Mexico, which had been decrypted by Knox (figure 2 overleaf). At that point the British advised the Americans against recruiting mathematicians. Instead, they should look for people with 'an active, well-trained and scholarly mind, not mathematical but classical'.[2]

During the interwar period the technology of encryption developed rapidly. The German engineer Arthur Scherbius unveiled the first Enigma machine. It was first marketed to banks, but soon the German armed forces started investing in it. In order to make the cipher system better suited for military use, it was made more advanced. The basic principle, however, stayed the same. The pressing of a key on the keyboard sent an electric charge through the machine's rotor which would turn on a light illuminating the encrypted letter. Then one of the rotors would rotate. This meant that pressing the same key several times consecutively, would give different outcomes, as the position of the rotors changed after every encrypted letter.[3] This is explored further in chapter 8.

Enigma was widely thought to be unbreakable, by Germans and British alike. However, it is well known that often when something is claimed so categorically to be one way, someone will prove it to be the other way. The first step came not through codebreaking but from espionage, when a disgruntled German civil servant, Hans-Thilo Schmidt, handed over plans of the military Enigma machine to France. The French intelligence services, just like their neighbours across the channel and to the east, were convinced that Enigma was impenetrable, making the information useless. Instead of keeping it themselves, they handed the intelligence over to their ally Poland. Taking a different approach to codes and ciphers from the



CLASS OF SERVICE DESIRED
Fast Day Message ☑
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM
NEWCOMB CARLTON, PRESIDENT

Check
Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
23610  18140  22260  5905   13347  20420  39689  13732  20667
6929   5275   18507  52262  1340   22049  13339  11265  22295
10439  14814  4178   6992   8784   7632   7357   6926   52262  11267
21100  21272  9346   9559   22464  15874  18502  18500  15857
2188   5376   7381   98092  16127  13486  9350   9220   76036  14219
5144   2831   17920  11347  17142  11264  7667   7762   15099  9110
10482  97556  3569   3670
```

BEPNSTOPFF.

Charge German Embassy.

Figure 2
The famous Zimmermann telegram
(US National Archives, no. 302025)

British during the war, the Polish put a number of mathematicians to work, the most famous of which was Marian Rejewski. It was this Polish breakthrough that was the first successful attempt to break the Enigma codes, and one that the British efforts were dependent upon.[4]

In Britain, while most cryptanalysts still saw the breaking of Enigma as a lost cause, Dillwyn Knox was pushing for co-operation with the Poles. He had stayed on in intelligence, working on his edition of Herodas on the side. His fellow classicists and King's College members Frank Lucas and Frank Adcock had also stayed on. Adcock made a particular impact through his work as a talent scout, and recruited a large number of young academics, among them Alan Turing. Following the example of the Poles, the British were now recruiting more mathematicians than ever before.

Knox was the only original member of Room 40 who made the transition from breaking messages encrypted manually to tackling machine ciphers. His work exploited the fact that however infallible a machine was, the human who operates it was not. When encoding a message on an Enigma machine, the operator must choose a three-letter message key that indicate how the rotors of the machines should be set for decoding. This key should be chosen randomly, but the human brain makes a poor random letter generator. Even if one tried, there is likely be a pattern. More often than not, the operator would pick three letters that meant something to him, for instance an abbreviated word or the initials of a loved one. These recurring message keys were identified by British cryptanalysts and dubbed 'cillies' by Knox, as the first one to be identified was CIL.[5] Knox himself specialized in breaking the Enigma used by the Abwehr, the German intelligence services, until his death in 1943.

While Bletchley Park is best known for the codebreaking efforts, the decrypted messages were also translated and interpreted there. Most persons engaged in this work were civilians or military personnel with a knowledge of German and other modern languages. However, among them were also classicists such as Elizabeth Greaves. She had joined the army's women's service, the Auxiliary Territorial Service (ATS) after graduating from Somerville College in Oxford in 1942. The women's services attempted to post people where their skills would be most useful, but they struggled to find a good placement for a classicist. The services sent her to 'a variety of postings and occupations, some of them interesting and some of them humiliating'.[6] She was finally posted at Bletchley Park, where she worked on German army and air force intelligence.

> Once I had become accustomed to the work, I found it both demanding and interesting, which was so wonderful after the things they had found for me before I joined The Park, that I soon found myself contented, busy, efficient and convinced that the work I did was really useful.'[7]

Although most employees at Bletchley Park worked on Enigma and other German ciphers, some tackled codes and ciphers used by Italian and Japanese forces. Patrick Wilkinson, a young classics fellow at King's College in Cambridge, had already been recruited by Frank Adcock during the summer of 1938.[8] He worked on Italian ciphers, primarily at Bletchley Park but also in Algiers. After the war, Wilkinson conducted research on Horace and Vergil and translated Ovid, Vergil and Cicero into English. Another classicist involved with Italian codes was John Chadwick, who is today remembered for his work on the decipherment of Linear B alongside Michael Ventris (see chapter 2). He came up to Corpus Christi College before the war to read classics, but enlisted in the navy soon after. His time at Bletchley Park was confined to the latter part of the war, when he learned and then translated Japanese. Most of his cryptanalytical work was done in Alexandria on Italian codes. Once, his team deciphered the Italian GIOVE/DELFO code faster than their colleagues in Bletchley.

After the war, this led to a strange moment in a supervision:

> At the beginning of 1946, when I returned as an undergraduate to Cambridge, I was sent to a supervision on Latin literature with Patrick Wilkinson, a fellow of King's and a well-known Latin scholar. His first words to me as I entered his room were: GIOVE DELFO. I gaped at him. It had never occurred to me that he was [one of] the men at Bletchley whose business it was to decipher the code, and that I had beaten him to it in Alexandria. I am glad to say that he never held this against me.[9]

The co-existence between the Bletchley classicists and their more scientific colleagues was not always peaceful. In Knox's case, the different frames of reference sometimes caused a breakdown in communication.[10] To some, such as Donald Michie, who studied classics as an undergraduate but later retrained as a geneticist and computer scientist, it seemed as if people from different academic backgrounds did not mix:

> There was a literary set in Bletchley, and I was fresh from a *wholly* arts education. There were these two cultures – the mathematicians' culture was another – I worked all my time in the mathematicians' culture but I retained, certainly for a year or two, quite a lot of social links to various classics dons and literary people.[11]

Nevertheless, classical languages were sometimes used in a playful manner. At lunchtime, the codebreakers would play rounders on the lawn, using a tennis ball and an old broom handle. 'Everyone argued about the rules and the dons just laid them down, in Latin sometimes,' recalled Barbara Abernethy, who worked as assistant to Commander Denniston, the head of GC&CS.[12] Others shared their knowledge. Among the many leisurely pursuits that were offered at Bletchley Park was a course in Latin.[13]

Many different reasons interplayed in the recruitment of classicists. The success Room 40 had had with classical recruits was certainly one. Another reason was that classicists were seen as a good choice for working on Italian codes. When he was recruited, John Chadwick was told, 'You say you know Latin – you shouldn't find much difficulty with Italian.'[14] classicists of the 1940s had usually studied Latin and Greek from an early age, and recruiters saw this ability to learn languages as an asset. When Chadwick studied Japanese, it was he and another classicist who came top of the class. The Japanese course was run in Bedford, close to Bletchley, and only took in classicists, as the course organizers were convinced that with this group of people they could get the best results.[15] John Tiltman, the head of the military section at Bletchley Park, became rather popular in Oxford and Cambridge as he was almost the only one interested in hiring classicists.[16] The reasoning was that classicists were already used to studying languages where ideas were expressed in very different ways from modern European languages, which made learning a language such as Japanese easier.

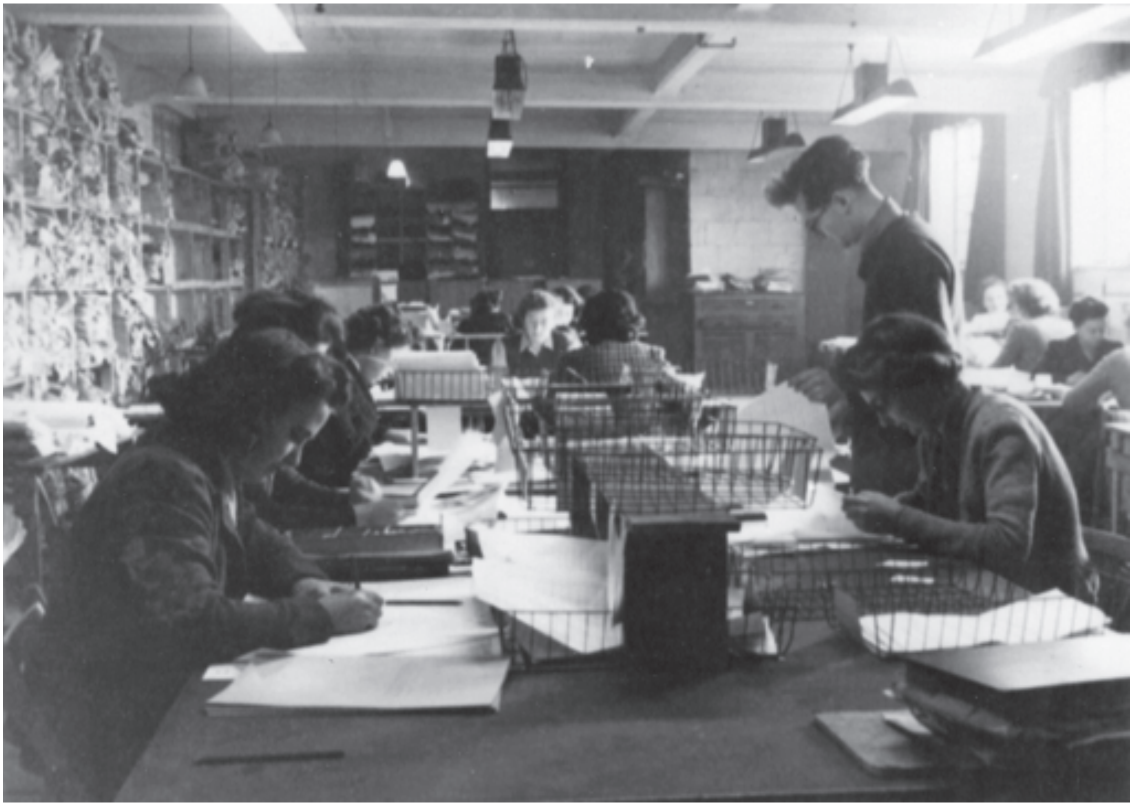


Figure 3
Working at Bletchley's Hut 6, the section that worked on the breaking of the Enigma machine codes
(By kind permission of the Bletchley Park Trust)

Another valuable skill developed by the study of classics was the ability to fill in gaps in texts. Patrick Wilkinson describes it as something classicists were taught by sitting exams which required translating passages that they had not seen before. The student 'has to guess, from his general knowledge and from the context, the meaning of unknown words'.[17] Knox used similar methods when breaking ciphers and reconstructing the text on papyri. Reconstructing a charred codebook is not so different from analysing a damaged scroll of papyrus, and vice versa. Just as he would when cracking a code, Knox would use better-preserved passages as a crib – a guessed plain text – which would help him decipher the copyist's poor handwriting.[18] In his book *The Decipherment of Linear B* (1958), Chadwick noted, without explicitly discussing his secret wartime service, 'There is an obvious resemblance between an unreadable script and a secret code; similar methods can be employed to break both.'[19] Michael Ventris, who ultimately deciphered Linear B (see chapter 2), would probably have fitted in very well at Bletchley Park, considering his extensive knowledge of both modern and ancient languages. However, he was never engaged in codebreaking, and instead served as a navigator in the RAF. It is possible that he was not picked for Bletchley as much of the early recruitment happened in small social circles, particularly at prestigious universities to which he had no connection.

Ultimately the technology of codes and ciphers advanced so quickly during the Second World War that classicists were no longer the excellent cryptanalysts they once had been. With more advanced encryption, the attempts at cracking that encryption had to evolve to keep up. At the beginning of the Second World War, all the cryptanalysts had to hand were pencil and paper, tools that took too long for the urgent business of codebreaking. By the end of the war, many ciphers were broken with the help of machines, such as the Bombe which went through possible Enigma settings, or the early computer – the Colossus – which was used to crack the high-level German teleprinter cipher Lorenz (see chapters 8 and 9). Both the preparation of raw data that went into the machines and the analysis of the output required considerable mathematical skills, and the running of the machines was seen as unskilled labour, which was often delegated to the women's services (figure 3).[20] A change in the way recruitment was done no doubt also influenced the number of classicists. Previously people had been recruited through social and academic networks, with the people at Bletchley Park often sharing similar backgrounds. It also meant that members of certain institutions were over-represented. During the war, a third of the fellows at King's College Cambridge served at Bletchley Park, presumably thanks to Adcock's recruitment efforts.[21] As the need for personnel grew and the organization changed character, the use of such 'old boys' networks' was no longer effective, and other means of recruitment was instead used.

Nevertheless, the impact that the classicists of Bletchley Park had on the war effort is undeniable. Dillwyn Knox's doggedness was key to the co-operation with Polish cryptanalysts, which was so important to the later British efforts that in turn were helped by the work of many younger classicists. The work at Bletchley Park was an interdisciplinary endeavour between civilians and military as well as between scholars of sciences and the humanities.

Part 2

The Second World War, Computers and the Future

7

The Joy of Breaking Codes

Christos Gkantsidis

In popular culture, the world of espionage is portrayed by death-defying spies that save the world at the nick of time by some act of unprecedented bravery. Reality is often more tedious, but equally exciting: the thrill comes from solving hard puzzles. Solving those puzzles comes after plenty of hard work by teams of experts, often of diverse skills. But what are these puzzles and what makes them difficult and, hence, exciting to solve?

In the case of espionage, the goal is to steal enemy's secrets. Those secrets can be instructions to platoons about the next attack, or details about how to organize the defensive line. The instructions have no value if they remain in the command headquarters; they need to be transmitted to the remote units that need to implement them. One plausible approach to guarantee the secure transmission is to entrust them to special agents, like those in the movies, and hope that they will not be intercepted. This approach is often not practical: there is a continuous stream of secrets that need to be transmitted, and a shortage of couriers that could guarantee secure delivery. It is far more convenient to transmit the instructions over a telecommunications system, for example by radio broadcasts or, in today's world, the Internet. But, this requires a way to transmit information securely over an *insecure* medium. Incidentally, securing the message is a good practice even when using couriers, as they are not always trustworthy, or they may even be captured.

Secure transmission of information over insecure communication channels is the domain of *cryptography*, literally writing in secret. With cryptography, the sender first transforms the original message so that it appears gibberish to anyone but the intended recipient; this process is called *encoding*. The recipient transforms the gibberish back to the original message, and this is called *decoding*. The sender and the recipient need to agree, ahead of time, the steps used for encoding and decoding; they need to agree on the *encryption algorithm*. Encryption algorithms are rather complicated: they may take years to develop and require scrutiny by many eyes to guarantee that they are indeed secure (or more precisely, that are not easy to break). It is, therefore, impractical to assume that the algorithm itself can stay secret.[1] Instead, the encryption process requires an algorithm, assumed to be known to everyone, and a secure *encryption* *key*, known only to the sender and the receiver.[2] The goal of *cryptography* is to devise encryption algorithms that make it difficult to recover the original message from the gibberish (the encrypted message) without possession of the encryption key. The difficulty in this context can be made very precise: the encryption algorithm is good if it requires testing all possible encryption keys to recover the original message.[3] For large enough sets of encryption keys, testing all possible keys is very difficult, even with the help of today's most powerful computers.

The need for secure encryption algorithms is not confined to warfare. In our Internet era we increasingly rely on communicating securely with remote entities, for example, to manage our bank account, to shop online or to talk to friends and family. We need strong guarantees that the website we visit is indeed our bank, our preferred shop or news agency; we also require that nobody can eavesdrop our conversations, or steal our personal data. The Internet's decentralized structure was paramount to its success,[4] but also made it a very hostile network: attacks can start from anywhere on the planet and can be made very stealthy. Indeed, malicious hackers from the other side of the world can be monitoring my web traffic without giving any clue of their presence.

Unfortunately for cryptographers (and the rest of us), we do not know of any *practical* encryption scheme for which we can prove that it is indeed difficult to break (difficult in the sense of requiring exhaustive search of all encryption keys). All current encryption algorithms rely either on (a) a transformation process that produces encrypted text from the original message and the key, which we call *block cipher*,[5] or (b) a mathematical operation that is considered to be very difficult to invert, called a *one-way function*.[6] Luckily there is growing evidence, but not certainty, that common block ciphers or one-way functions are indeed difficult to break (even assuming computers of the future). However, constructing a secure *cryptographic system* is much more than picking a secure block cipher or one-way function. Those building blocks need to be composed in a deliberate way to construct a functional system for transmitting messages, and the resulting system needs to be used (often by non-expert users) without violating the security assumptions that were put in the design.

Cryptanalysis tries to identify problems in the block cipher, the one-way function, the composition of the encryption blocks, or even the way that the encryption device is typically used. Those problems or misuses may give clues on how to reduce the secret key search space; the hope is that with enough computing machinery it should be possible to search the reduced key space efficiently (see chapter 8). It is worth mentioning that cryptanalysis is not the only way to steal secrets; modern-day hackers also look for vulnerabilities in the software that implement the cryptographic system (software bugs),[7] or even the interaction of the crypto software with the computer to identify ways to extract the secret key or message.[8]

Going back to the espionage world: if your enemy uses encryption, as the Axis did in the Second World War, are there any chances of decrypting their messages without possession of their secret keys? This is the puzzle that many cryptanalysts working for the Government Code & Cipher School (GC&CS) at Bletchley Park (UK), at Station Hypo in Hawaii (USA), and elsewhere tried to solve at that time. It should be appreciated that the Germans in particular used relatively advanced encryption machines for their era, and that many tools of cryptography and cryptanalysis that we take for granted today were unknown at the time. Those teams had to make significant progress in the understanding of cryptographic codes, in developing cryptanalysis techniques and building computers to rapidly test candidate encryption keys (arguably the first electronic programmable computer, Colossus, as discussed in chapter 9).

Cryptanalysis transformed intelligence gathering[9] and gave a significant advantage to the Allies during in the Second World War. After the war GC&CS changed its name to Government Communications Headquarters (GCHQ) and continued to work on cryptography and cryptanalysis. The US also intensified their efforts by strengthening the agency currently known as the National Security Agency (NSA). GCHQ, NSA and other similar entities remained relatively hidden from the public during the Cold War. (It was because their work was secret that NSA is jokingly referred as 'No Such Agency'.) Their respected governments only belatedly acknowledged in public the contributions of those agencies and of the individuals working for them. Even more unfortunately, many innovations that took place inside those agencies also remained hidden and had to be rediscovered.

For example, the work by Flowers and his colleagues on Colossus did not influence the design of general purpose computers; that honour goes to ENIAC, which appeared a few years after Colossus.[10] Alan Turing is well known for his theoretical work on the Turing machine (a mathematical model that helps us understand the limits of what is computable[11]) and his work on artificial intelligence (the Turing test[12]); his design and engineering work on Bombe and Delilah (a speech security system) were hidden from public until the mid-1970s.

The stream of innovations that were kept secret continued during the Cold War as well. Among the most famous is the idea of using different keys for encryption and decryption by James Ellis of GCHQ in 1969.[13] Public key cryptography was later reinvented by R. Rivest, A. Shamir and L. Adleman[14] and W. Diffie and M. Hellman,[15] and today is the basis for secure Internet communications.

The next chapters narrate in more detail the birth of modern cryptanalysis and cryptography during the Second World War and beyond. Prior to the First World War cryptography relied on using codebooks: human operators had to open physical books to search for the codes necessary for encryption and decryption. This was a manual process that by necessity could not provide strong encryption. The cryptanalysts of the time used statistical methods and plenty of guesswork to revert the encoding process (often, they also relied on luck or heroics to recover those codebooks). Between the two world wars, we see the advancement of electro-mechanical machines for cryptography (rotor machines), which simplified the job of the human operators and increased the complexity (and security) of the encryption process by a quantum leap. Breaking those machines was the big challenge for the cryptanalysts of the time. To that end, they invented new approaches to identify and exploit weaknesses of the new cryptographic machines (even without having descriptions or access to them!), and built machines that resemble today's computers to automate code breaking.

8

Alan Turing and the Enigma Machine

James Grime

By the end of the Second World War 9,000 people had worked at Bletchley Park, the top-secret codebreaking facility that was initiated as the Government's Code and Cipher School (GC&CS) in September 1939. These codebreakers were made up from a collection of mathematicians, linguists, lawyers and engineers, as well as classicists as we have seen in chapter 6, while some were just people who were good at games and puzzles.

Many of them thought the Enigma code to be unbreakable: it was certainly incredibly difficult, but there was one who still thought the problem was worth tackling, a brilliant young mathematician called Alan Turing. His contributions to Bletchley Park cannot be overstated. His ideas made breaking Enigma possible, including the design of a large mechanical machine, called the Bombe, that could determine the daily Enigma settings in under twenty minutes.

Within the sciences, Alan Turing's reputation goes beyond that of his Second World War work. His work in computing, artificial intelligence and biology means Turing is considered one of the twentieth century's greatest mathematicians.

Young Turing

Alan Mathison Turing was born on 23 June 1912. His mother came from a family of engineers, and his father was a civil servant in British India.

As a boy Turing was fascinated by the natural world and how things grow. At some point Turing received a science book, written for children, called *Natural Wonders Every Child Should Know* by Edwin Tenney Brewster. This book was radical in the way it explained its concepts to children in a grounded and accessible way. It explained how the body was made from building blocks known as cells, and how animals grow from these cells. This book introduced Turing to science and proved to be a great source of inspiration on his life.

At the age of thirteen Turing started attending Sherborne School, in Devon. Turing was a bright student, but sometimes struggled to see the value in subjects outside of maths and science, with his headmaster remarking in one school report:

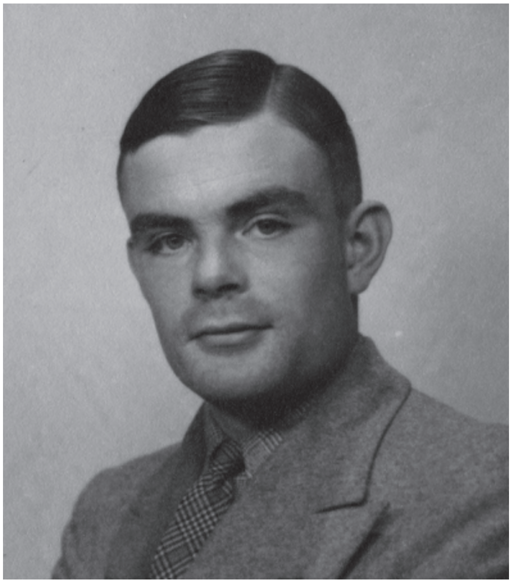


Figure 1
A passport photograph of Alan Turing of unknown date (Reproduced by kind permission of King's College Library, Cambridge, AMT/K/7/9)

> I hope he will not fall between two stools. If he is to stay at a Public School he must aim at becoming educated. If he is to be solely a scientific specialist, he is wasting his time at a Public School.

Turing's love of science was not really shared by the other boys either: they found his experiments annoying and smelly. One pupil who did share Turing's enthusiasm for science was Christopher Morcom, a boy in the year above Turing, who has been described as Turing's first love.

It was Morcom who introduced Turing to his favourite chemistry experiment, the 'iodine clock reaction'. In this experiment two colourless solutions are added together, one containing starch and sodium thiosulfate, the other containing potassium iodide. When these are mixed, nothing appears to happen for a few seconds, until the solution suddenly turns dark blue. The effect is quite dramatic. By changing the proportions of the different chemicals, you can change the timing of the colour change.

Unfortunately, Christopher Morcom died at the age of eighteen after complications following bovine tuberculosis. Morcom's death affected Turing deeply. The school set up a science prize in Morcom's name, and it is fitting then that the first recipient of the Christopher Morcom Science Prize was Alan Turing himself, for his investigation into the iodine clock reaction.

Turing's prize was a copy of the book *Mathematical Recreations and Essays* by W. W. Rouse Ball. This book has influenced many generations of mathematicians, containing chapters on magic squares, the four-colour theorem and other classic mathematical problems.

The last chapter of the book may have particularly intrigued a young Alan Turing as it was about codes and codebreaking. Turing's own favourite code from this chapter was one of the simplest. It is known as a Grille cipher, and involves placing a piece of card with holes over some normal text with the letters through the holes spelling a secret message, something he often did with school friends.

Alan's teachers began to recognize him as a potential mathematical genius and after leaving Sherborne, Turing matriculated at King's College and studied mathematics at Cambridge.

The Enigma machine

At the beginning of the twentieth century it had become possible, and indeed necessary, to mechanize encryption.

The Enigma machine was invented by a German engineer called Arthur Scherbius in 1918. Early versions were sold to businesses such as banks and railways. However, these machines were quite expensive and did not sell very well. Then in 1925 the German navy started to use them, followed by the army and air force. By 1930 a new version of Enigma, known as Enigma I, had been created just for military use.

Enigma looked a lot like a typewriter, but unlike a typewriter had no carriage or paper (see figure 2). Instead there was a second set of letters wired to light up. For example, if one typed a simple message into Enigma such as HELLO, this might be encrypted as ILBDA. This code was then written down and transmitted by radio. But notice that the two Ls in the message above have become two different letters in the code. Enigma encrypted each letter of the message using a different code, which is what made Enigma so difficult to break.

The changing code came from three wheels inside the machine, known as rotors. These rotors turned as you typed: there was a fast rotor that turned after every letter, a middle rotor and a slow-moving rotor. The action was similar to hands on a clock.

Inside the rotors the machine is full of criss-cross wiring; pressing a letter on the keyboard creates a circuit connecting the battery to a light. However, when the key is pressed again, the rotor moves, which means that all the wires rotate one place forwards and connect the battery to a different light, creating a different code letter.

Each rotor has twenty-six starting positions, and the rotors themselves could be taken out and put back in a different order. At the front of the machine was the plugboard, consisting of wires that acted as an extra level of scrambling, something that was only available on the military Enigma machine. During the Second World War Enigma had a total of 159 million million million settings, and these settings changed every day.

However, it was quite simple for a German operator to decrypt any message they received. The second operator would have an Enigma machine as well, which was set up in exactly the same way as the first machine. The daily settings would be written down for the operator on a piece of paper known as 'key sheets'. To decrypt the message the operator would type the code into the machine, and the letters from the original message would light up.

For added security, each message would be encrypted using its own

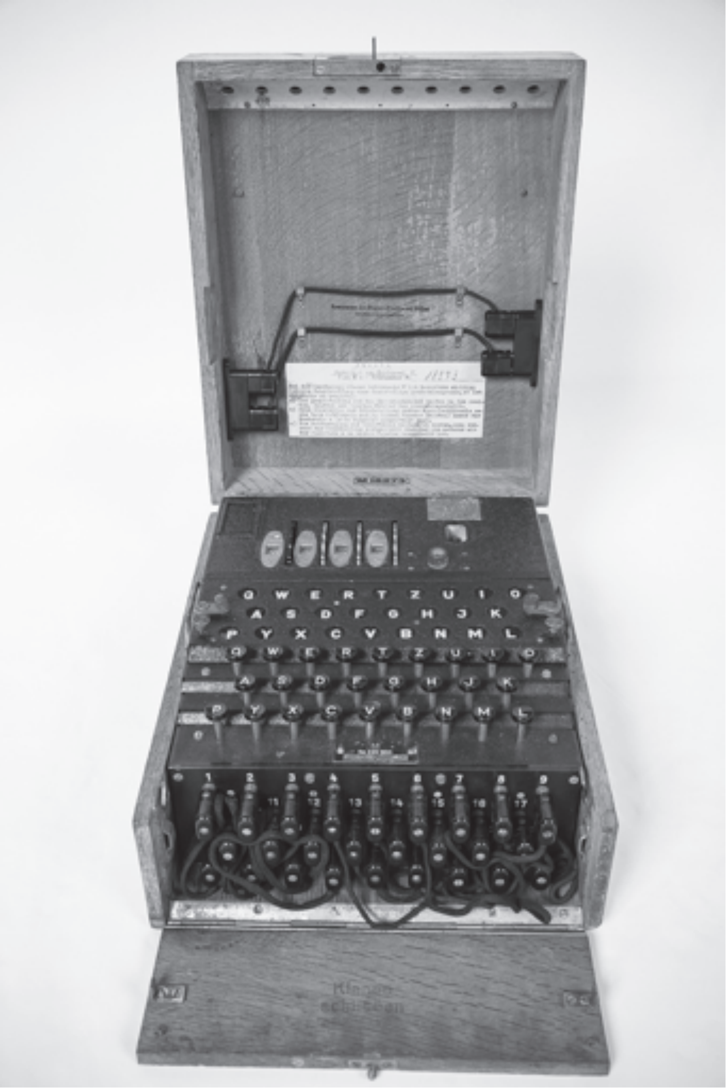


Figure 2
The Enigma Machine. This model, on loan to the Fitzwilliam Museum from GCHQ, is an Enigma M4 – a rare four-rotor Enigma machine used on U-boats from 1942 (© Crown Copyright 2017)

rotor starting position, a triplet of letters known as the 'message key'. This setting could be chosen by the operators themselves, but would have to be put at the start of the message – in code.

To encrypt the message key, the operator used the Enigma machine itself. First, the operator would set his machine according to the key sheet. The operator then picked his own secret setting, say ABC, and would type that into the Enigma machine twice. This produced six letters in code that were placed at the start of the message. The second operator would use his Enigma machine to decode those six letters and get ABCABC, and this would reveal the secret setting to use for the rest of the message.

Enigma was incredibly difficult to break, but the first to do so were the Polish, years before the war started.

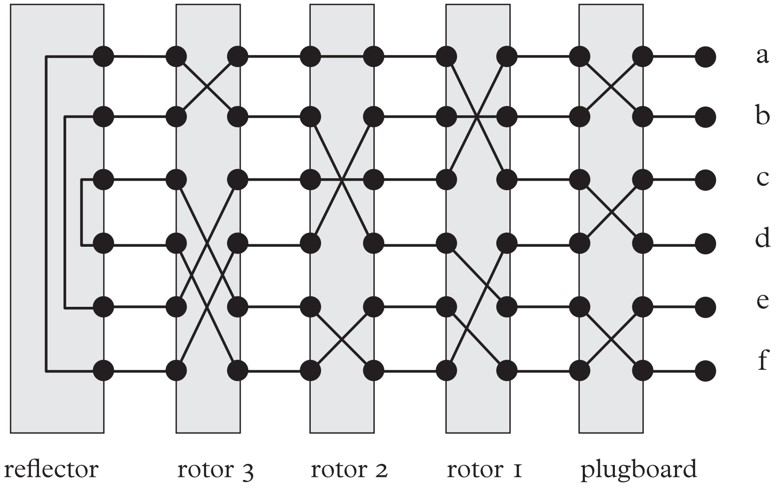


Figure 3
A simplified example of the wiring inside Enigma. Here, pressing the letter 'a' will connect to the letter 'e' which will then light up
(Drawing by T. Richardson)

The Polish codebreakers

Before the Engima machine was devised, codebreaking had been seen as a language problem. But Enigma was a technological problem that needed a technological solution. Therefore in 1932 the Polish Cipher Bureau, who already knew Germany was a threat, started to recruit bright young mathematicians such as Marian Rejewski, Henryk Zygalski and Jerzy Różycki.

The first problem to solve was how the machine worked. The cipher bureau had obtained a commercial Enigma machine, but this was different from the military version. It did not have a plugboard and the rotors were wired up differently inside. Remarkably, Rejewski managed to deduce the wiring of the military machine without ever seeing the machine itself. After that the Polish could make their own replicas. Contrary to popular belief, the machine itself was never the mystery. The mystery was to identify which *setting* was being used on a given day. This was something that had to be worked out every day.

The Polish codebreaking methods concentrated on the message key, the six letters of code at the beginning of each message. This little code, made using Enigma itself, was simply a repeated triplet of letters as we have seen. This meant that the first and fourth letters were the same, as were the second and fifth letters, and third and sixth letters. This was a clue, and acted like a fingerprint, revealing the Enigma setting for that day. At one point it was estimated that the Polish were breaking 75 per cent of Enigma messages they received. But each time the Germans increased security, the Polish would be back to square one. It was a constant battle.

Finally, in 1938, they produced a codebreaking machine called 'Bomba'. This machine was small enough to sit on a desk, and worked like six Enigma machines working simultaneously, still working on breaking the six-letter message key. There were six ways to arrange the three rotors, meaning the Polish needed six Bomba machines.

Then, the Germans increased security again. Although still unaware of the Polish efforts, the Germans increased the number of rotors so that they were now picking three from a choice of five. There were sixty ways to do that, which meant the Polish would need sixty Bomba machines. The Polish did not have the resources for that, and so, five weeks before Poland was invaded, there was a secret meeting between the Polish and the British codebreakers.

The 'father of computing'

While the Polish codebreakers were tackling Enigma in the 1930s, Turing was still at university. It was while he was studying for his Masters degree in 1935 that Turing decided to take on one of the great unsolved problems in mathematics – and changed the world.

At the turn of the century a German mathematician called David Hilbert had set out a series of challenges to twentieth-century mathematicians. This was a list of what he considered to be the most important unsolved questions at that time. One of these problems was known as the *Entscheidungsproblem* – the Decision Problem. The problem was to establish whether there a general method that can decide whether a mathematical problem was provable.

Turing learnt of this problem while attending lectures at Cambridge. He thought that, since this was a method that can be simply applied to any mathematical statement, it was the sort of thing that could be done by a machine without need for human intervention. Turing then began to define a general type of machine that could do any calculation a man could do. This computing machine could read symbols on a tape, and then add or delete symbols according to instructions. Furthermore, those instructions could be fed to the machine on the tape itself, meaning the machine could change its function. This idea was the beginning of what we now call computer science.

Turing eventually solved the problem in the negative: there was no general method to decide whether any given statement was provable. You can imagine, then, that Turing must have been more than a little disappointed when he discovered that someone else had come to the same conclusion before him. A Princeton mathematician called Alfonzo Church had also disproved the Decision Problem just a year earlier. However, Church's method was far more complicated than Turing's and it is Turing's more intuitive, practical approach that is taught today.

In 1936 Turing went to Princeton to start his PhD with Church as his supervisor. Even during this time Turing maintained an interest in codes. In a letter he wrote to his mother from Princeton, Turing mused on what would be the most general type of code, thinking his ideas might be of interest to the British government. When Turing returned to Cambridge in 1938, he turned his attention to one of the other great unsolved problems in mathematics, the zeros of the Riemann zeta function (see plate 19).

Bernhard Riemann had identified this mathematical function in 1859. It is difficult to explain in laymen's terms, but essentially it concerns the relationship of zeros with the distribution of the prime numbers. Calculations to find the zeros were at that time done by hand, but in 1938 Turing had already designed and begun to build a machine that could calculate the zeros of the zeta function much more quickly (figure 3).

Unfortunately, the project was interrupted by the outbreak of the Second World War. The very day after war was declared, Turing reported for duty at Bletchley Park.

Turing at Bletchley Park

Initially Turing was part of a small team of codebreakers including linguists such as John Tiltman and Dilwyn 'Dilly' Knox, and other mathematicians such as Peter Twinn and Gordon Welchman. This group worked in the atmosphere of a university research group, comprised as it was of academics from Oxford and Cambridge both young and old. The question they faced was simply, could Enigma be broken?

This question was answered a few weeks before the war when representatives met with the Polish codebreakers. Not only did they receive information about how they were getting on with breaking Enigma, but they also obtained a couple of the Polish Enigma replicas. But there were still some major problems.

The first problem was that the Polish methods depended on the six coded letters at the beginning of each message, which was the repetition of the message key. If the Germans stopped repeating this setting, then the Polish methods would no longer work. The second problem was that by this time the German navy was not using Enigma machine itself to encrypt the message key; instead they had devised a separate code book for their use that the Polish had not broken.

What the British needed was a new method to break Enigma, one that would be able to replace the Polish methods if the Germans changed procedures, and ideally one that would work for army, air force *and* navy messages. Before long the workload was divided up, and Turing was put in charge of Hut 8, the section responsible for breaking the navy Enigma.

While at Bletchley, Turing developed a reputation for being a bit of an eccentric. There are stories about him cycling to work wearing his gas mask as a way to avoid hay fever, and of him chaining his mug to the radiator so no one else would use it. He was also known as 'The Professor', despite only being twenty-eight at the time, and his treatise on Enigma, which was required reading for new members of the team, was known as 'Prof's Book'.

Turing was also a very talented long-distance runner, and would run for meetings from Bletchley Park to London, a distance of forty miles. He was seriously considered for the 1948 Olympics, though an injury prevented his enrolment.

While at Bletchley Turing became great friends with Joan Clarke, a mathematician who worked with him in Hut 8. Turing would arrange his shifts to coincide with hers, and he soon proposed to her. Not long after the engagement Turing revealed to her that he was a homosexual;

despite that the engagement lasted until the summer of 1941, when it was finally called off. Turing obviously had been guarded about his sexuality, particularly during his time at Bletchley Park.

He continued meanwhile to work on the problem of the naval Enigma. He had deduced the navy procedure, and partially reconstructed the code books the navy were using. This was later confirmed by code books stolen from U-boats. Turing also developed a statistical method for determining which rotors were being used that day. This would reduce the number of potential rotor orders from hundreds to just a few, vastly speeding up the codebreaking process. The problem now was to deduce the other Enigma settings, such as the plugboard and rotor positions. He then immediately started working on the design of his Bombe machine.

The Bombe was much larger than the Polish Bomba machines, and was designed to deduce the daily Enigma settings in a way that did not rely on the repetition of the message key (see figure 4). Instead, the codebreakers would try to guess a word or a phrase that might appear in the code; these guesses were known as 'cribs'. A good source of cribs was the early morning weather forecasts that were transmitted to German ships.

For example, we could try to find the phrase 'weather forecast', *wettervorhersage* in German, in the code below:

```
…G K X T P Q V M F P A O W L R J C H S B …
      W E T T E R V O R H E R S A G E
```

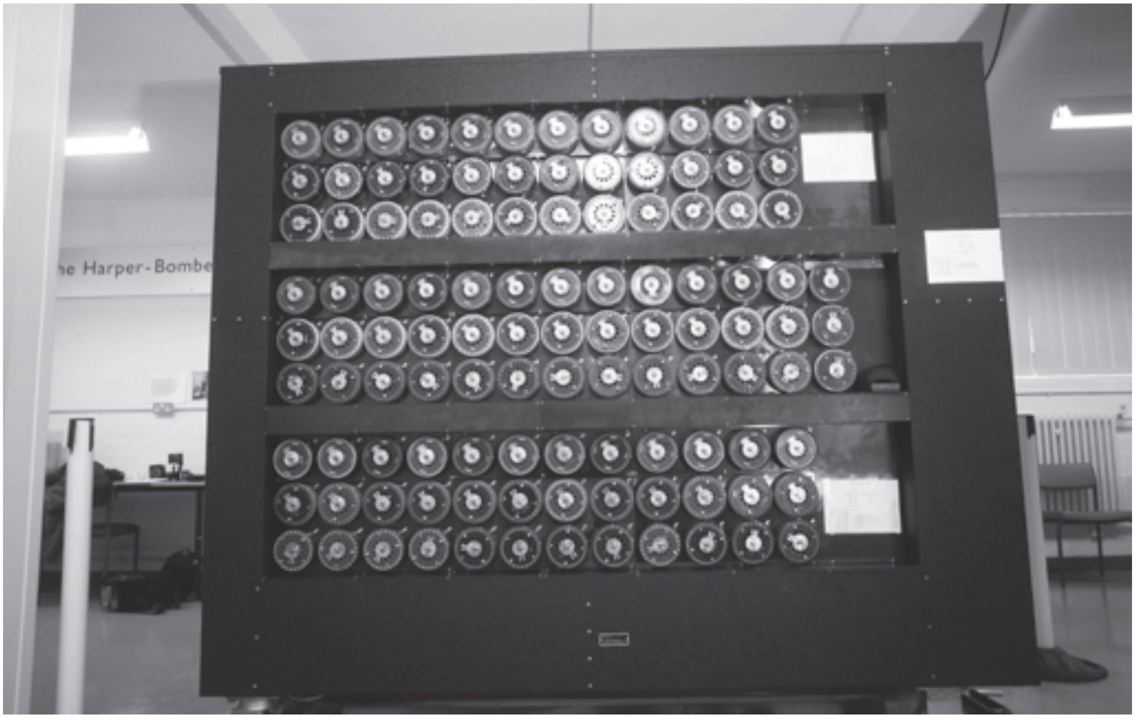


Figure 3
The replica Turing-Welchman Bombe machine displayed at Bletchley Park
(Reproduced by permission of the Turing Welchman Bombe Rebuild Trust)

Although there seems to be no clue to find the correct position for the crib, there was in fact a small flaw in the machine. Because of the way Enigma was designed to code and decode, a letter could never become itself. That meant no letter of the crib could match with the code, as that would be impossible. Once you have found a position that works, you need to find the Enigma setting that makes that part of the code say '*wettervorhersage*'. This is essentially what the Bombe did.

The Bombe was actually a process of elimination. The Bombe operator used wires at the back of the machine to input a letter of the code corresponding to a letter in the crib, according to the instructions given by the codebreaker. The machine would then run. Each level of the machine worked like twelve Enigma machines operating simultaneously, making deductions about the plugboard and rotor position. However, it was faster to reject the wrong settings than to go looking for the right settings. When a setting was rejected, it allowed a whole class of settings to be rejected at a stroke. Anything that could not be rejected caused the machine to stop, and the setting could be checked.

In this way the Bombe machines could check through the Enigma settings in under twenty minutes. The first Bombe machine was delivered to Bletchley Park in March 1940 and around 200 machines were finally built for codebreaking purposes. In May that year the Germans finally stopped repeating their secret message keys, as had been anticipated, and so Turing's Bombe machines were used to break Enigma messages for the rest of the war.

After the war

After the war Turing was recognized for his work at Bletchley Park, receiving an OBE, although the reason why he received the award (which he subsequently kept hidden away in a box) was not made public.

He continued his work in computing after the war, first at the National Physics Laboratory in London, and then at the University of Manchester. Indeed, one of Turing's first uses of Manchester's Mark 1 Electronic Computer was to find the zeros of the Riemann zeta function, a project of his that had been interrupted by the outbreak of the war.

Later, in 1951, Turing turned his interest to biology, in particular the patterns of animal skins, engaging with questions such as why cows have patches, zebras have stripes and leopards spots. To answer this particular question, Turing modelled the chemical processes that create the colour variations. He assumed that these patterns were the result of two chemical mechanisms, one that causes colour and a second that inhibits it. He worked out that these processes propagate by diffusion but, instead of turning the animal all one colour, the two processes stabilize into long-lived patterns.

The equations in Turing's model were similar to ones used in physics to describe waves, which lead Turing to describe the phenomenon as 'waves on cows and waves on leopards'. Turing's work remains seminal in mathematical biology, yet it was as a child that he had first become fascinated in such things.

Turing's brilliant scientific mind and promising career came to an abrupt end in 1954. After a break-in at his Manchester home, Turing admitted he was homosexual to Manchester police, and he was subsequently arrested and convicted of what was termed 'gross indecency' with males in 1952. He lost his job as a consultant for the codebreakers and he was now barred from going back to the USA. What was worst, though, was that he was subjected to a hormone treatment, a 'treatment' practice of the times with severe physical and mental side effects. In 1954 Turing died from cyanide poisoning, which was determined by the authorities to be suicide. He received an official apology from the British government in 2009 and eventually a posthumous pardon in 2014.

The work conducted at Bletchley Park involved a range of expertise from many people in many disciplines. But it was Alan Turing who thought Enigma could still be broken when others had given up. The breaking of Enigma would prove to be vital in the Battle of the Atlantic, allowing food and supplies to cross the ocean from the USA. Turing's non-conformist attitudes and ways of thinking proved to be years ahead of their time, and changed the world.

9

Breaking the Lorenz Cipher Machine: The Other German Code Machine

James Grime

Colossus is arguably the world's first programmable digital computer, built in secret in the Second World War to break German codes (figure 1).

However, Colossus was not built to break Enigma, the infamous code machine used by the German soldiers of the Second World War. Instead it was built to break an even harder German code: a cipher machine called Lorenz. This code was many times more complex than Enigma and was used by the top level of German High Command, including Adolf Hitler.

The team that broke Lorenz was a small group of mathematicians, engineers and linguists, who each brought their different skills to the problem. Breaking Lorenz may have seemed impossible, yet not only did this team achieve to break the code, they were able to do it without ever seeing the machine itself.

Breaking Lorenz complemented the work done in breaking Enigma. Whereas the majority of messages were coming from Enigma, Lorenz provided insight into the German grand strategy. Hitler called the machine his 'Secrets Writer' and considered it unbreakable.

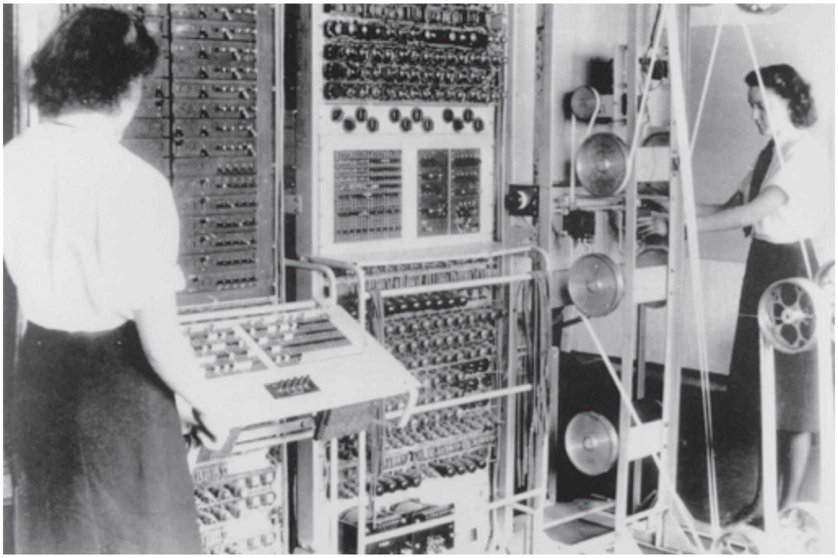


Figure 1 The Colossus codebreaking computer in operation, 1943 (The National Archives (UK), document record FO850/234)

Breaking Lorenz is a story of determination and ingenuity that not only equals that which broke Enigma but has been described as the greatest intellectual achievement of the entire war.

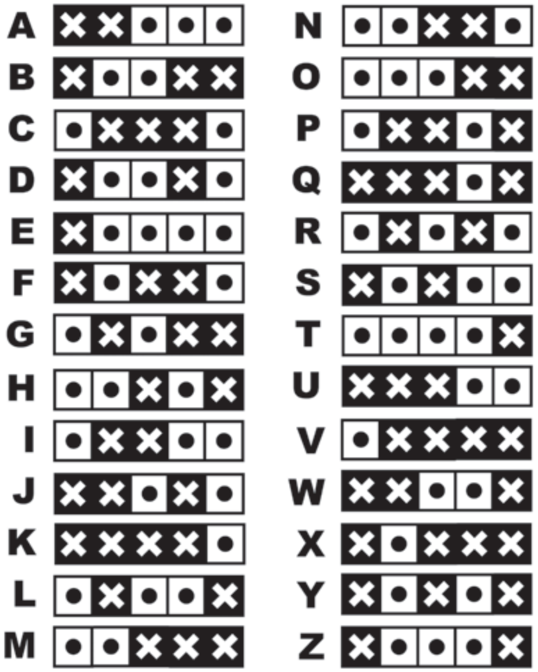
The Lorenz cipher machine

Today every message on the Internet, be it an email or a tweet, is transmitted using ones and zeros; it is easy to picture this as a type of Morse code. However, before the invention of the Internet, teleprinters were used. These transmitted messages in much the same way as it is done today. A message was typed on the teleprinter, which would then convert it into electrical impulses and transmit it by wire or radio. At the other end those electrical impulses would be punched on to tape.

Each letter was transmitted using five pulses and blanks. This teleprinter code (or Baudot code) was written using crosses and dots (figure 2). One manufacturer of teleprinters was the German-based Lorenz company. However, there was nothing secret about teleprinter code. Any messages sent in this way could be easily intercepted and read by the enemy.

To allow people to send encrypted messages, the Lorenz company sold a separate cipher machine to attach to the teleprinter. This cipher machine was quite large and heavy. It was made of twelve wheels that would generate and add 'obscuring letters' to the message.

Adding obscuring letters worked as follows. The Baudot letters are made from combinations of five crosses and dots. Suppose the letter M was required: the cipher machine would then generate a random letter, for

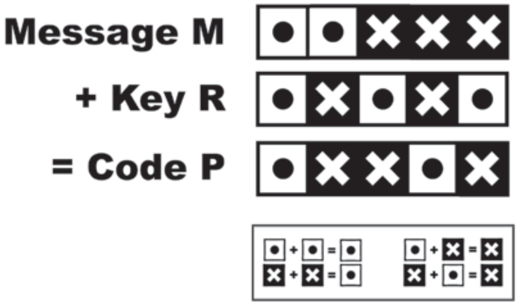


A	×	×	●	●	●	N	●	●	×	×	●
B	×	●	●	×	×	O	●	●	●	×	×
C	●	×	×	×	●	P	●	×	×	●	×
D	×	●	●	×	●	Q	×	×	×	●	×
E	×	●	●	●	●	R	●	×	●	×	●
F	×	●	×	×	●	S	×	●	×	●	●
G	●	×	●	×	×	T	●	●	●	●	×
H	●	●	×	●	×	U	×	×	×	●	●
I	●	×	×	●	●	V	●	×	×	×	×
J	×	×	●	×	●	W	×	×	●	●	×
K	×	×	×	×	●	X	×	●	×	×	×
L	●	×	●	●	×	Y	×	●	×	●	×
M	●	●	×	×	×	Z	×	●	●	●	×

Figure 2
Baudot teleprinter code
(Drawing by J. Grime)

example, R. This random letter is also known as the key. The symbols of these two letters were then added together, pair by pair, using the rule that if the two symbols are the same they make a dot, and if the two symbols are different they make a cross.
In this example, adding R to the letter M creates five crosses and dots that correspond to the letter P in teleprinter code. This is the code letter that is then transmitted.

At the other end, the receiver of the code has a Lorenz cipher machine too. This machine is set in exactly the same way as the first machine. This causes the second cipher machine to generate the same sequence of random letters as the first.



In our example this will mean the receiver will generate the same key letter R. The second machine will then add that to the received code letter P. Using the same rule for adding teleprinter symbols as before, adding R to the letter P will result in the letter M – the original message. In other words, adding the key twice cancels itself out.

The effect of the Lorenz cipher was similar to Enigma. Pressing a letter repeatedly would create different code letters. At the same time the machine would cancel itself out which means two machines set the same will code and decode. However, Lorenz was far more complex than Enigma.

Enigma was made from three wheels and when the wheels moved (as they did for every letter of the message) then the code changed. These wheels moved like clockwork – the rightmost wheel moved every time. When the rightmost wheel had done a full turn, it would kick the middle wheel one place forwards. When the middle wheel did a full turn, it would kick the leftmost wheel one place forwards. Each wheel had a period of 26 letters. This meant the pattern did not repeat until all three wheels were back to their original starting position.

On the other hand, Lorenz was made from twelve wheels which moved in a far less predictable pattern. Each wheel had a different period that ranged from a period of 23 letters to a period of 61 letters. These periods had been designed in such a way as to make the time until all wheels were back to their original positions as long as possible. Evenly spaced on the outside of the wheels were pins, essentially on/off switches that caused the wheel to generate a pulse when in a position with a pin set to on.

The five rightmost wheels of the Lorenz cipher machine were known as the chi-wheels. Together these wheels generated five pulses or blanks and then after each letter all moved one place forwards. The five leftmost wheels were known as the psi-wheels. Together the psi-wheels generated another five pulses or blanks which were added to those generated by the chi-wheels to create the final key letter. The movement of the psi-wheel was less regular and was controlled by the final two wheels in the middle known as the motor-wheels.

The Lorenz settings were written down for the operators in code books. Altogether there were 501 pins on the wheels, with around half set to on and half set to off. This pattern of on/off pins changed once a month. The wheel position was chosen from another book, and changed for every message. At the start of each message a number was transmitted which the receiver would look up in their book in order to set their wheels to the same positions.

To grasp fully how difficult Lorenz was, one needs to think that the number of ways to set the Enigma machine was already vast: as we have seen, 159 million million million – i.e. 159 with eighteen zeros after it – far too many settings to ever check by brute force. On the other hand, the total number of ways to set up the Lorenz cipher machine was 100 followed by 168 zeros, an astronomical number of combinations!

One big difference between Lorenz and Enigma was the way they were used. Enigma was relatively portable, and used by the servicemen themselves. It has been estimated there were as many as 40,000 military Enigma machines around the world. But Lorenz was different. These machines were not portable; they had to be located in secure places near Berlin and field headquarters in Russia, the Middle East and France, creating a network of around twenty machines. These machines were only used to send the most important messages between members of the German High Command.

Meanwhile, although British listening stations were able to pick up German teleprinter traffic, they had no idea what it meant. Hence these messages were sent to Bletchley Park's research section, where the specialist mathematicians and linguists were trying to break codes that had not yet been broken – including Lorenz.

At first, this Lorenz teleprinter code was a complete mystery to the researchers at Bletchley Park. Without having seen the machine that made it, and with no knowledge of its structure, it seemed like an impossible task to break this code. That was until one disastrous mistake by a single German operator.

The mistake that cracked Lorenz

In late August 1941 an operator used the Lorenz cipher to send a message from Athens to Vienna. This message was quite long, consisting of around 4,000 characters. However, something went wrong and the operator at the other end did not receive the message and asked for the message to be transmitted again.

Annoyed at having to send this message again, the first operator reset his machine and started to send the message again – but this time with a few abbreviations – just to make the message a little bit shorter. This meant that the codebreakers at Bletchley Park effectively had two copies of the same message sent on the same setting, but with a few differences. It was chief cryptographer of the Government Code and Cypher School (GC&CS), John Tiltman, who first exploited this mistake.

Lieutenant Colonel John Tiltman (later brigadier) was a legend in his own time. First as a linguist, and then as a cryptanalyst, Tiltman served in two World Wars. In 1939 Tiltman tackled the code being used by the Japanese navy and had set up a cipher school to train more recruits. He was neither a university graduate nor a mathematician, and was not fully comfortable with the new era of machine ciphers, preferring to tackle the more traditional, hand-made systems. Nevertheless Tiltman is considered one of the greatest code breakers of his era.

In the early days of Lorenz, the wheel position was transmitted at the beginning of each message using twelve letters. So Tiltman could be sure that the two messages from Athens had been sent using the same key. This meant that if Tiltman added the two codes together, using the usual rules of teleprinter addition, then the keys would cancel out. The result was now the sum of the two original plain-text messages. Assuming this is the same message with a few abbreviations, Tiltman was able to painstakingly piece together the original message. It took him ten days.

The message itself was not particularly useful or insightful, but by subtracting the plain text from the code, this meant they could also work out the key. This was extremely important and gave them a long example of a key generated by the Lorenz cipher machine. It was hoped that from this key they could determine something about the structure of the machine that made it. Eventually, after others had failed to find anything useful from the key, in October 1941 it was given to a rather junior member of the team, Bill Tutte.

Bill Tutte in Cambridge

William Thomas Tutte was born in Newmarket, near Cambridge on 14 May 1917. His father was a gardener and his mother a housekeeper. At school he was interested in science and mathematics, winning a scholarship to Cambridge and County High School for Boys, which meant an eighteen-mile commute for the young boy. In October 1935 Tutte matriculated to Trinity College, Cambridge to read chemistry (figure 3 overleaf). Despite this, Tutte remained interested in mathematics, continuing to sneak into maths lectures and joining the Trinity Mathematical Society.

It was at the mathematics society that Tutte was introduced to a problem that lead to his first published paper. This was the 'squared square' problem – can a square be made from other squares of different sizes? This was no more than a fun puzzle for maths enthusiasts, but remained unsolved up to that point.

Tutte worked on this problem with three other society members: Arthur

Figure 3
Bill Tutte as a student at Trinity College, Cambridge (Photograph by permission of The Master and Fellows of Trinity College Cambridge,ref. FA II.34 [2])

Stone, Cedric Smith and Rowland Brooks. While trying to solve it, the four students found a remarkable connection between squared squares and electrical networks.

No one would have guessed that such completely different problems were related, but this insight allowed them to create some of the first squared squares. The four students published their paper in 1940, and Tutte later credited this problem as his training for his career in mathematics. The smallest squared square possible is made of twenty-one other squares of different sizes, and is now the logo of the Trinity Mathematical Society (see figure 4).

The solution to this problem may have been what lead Tutte to be recommended to GC&CS. After completing his Masters in chemistry in 1941, Tutte was sent to code breaking training and assigned to the Research Section at Bletchley Park.

Reconstructing the Lorenz machine

It was the head of the research section, Captain Morgan, who gave Tutte the problem of the key – maybe because he knew that Tutte was the sort of person who liked puzzles. While thinking about the problem, Tutte would stare off to the middle distance – he later remarked that his colleagues may have doubted that he was doing anything at all. However, to find a pattern in the key Tutte decided to apply something he had learned from his codebreaking training.

A secret message can use a different cipher for each letter of the message. If that pattern repeats, for example, if you use five ciphers and that pattern

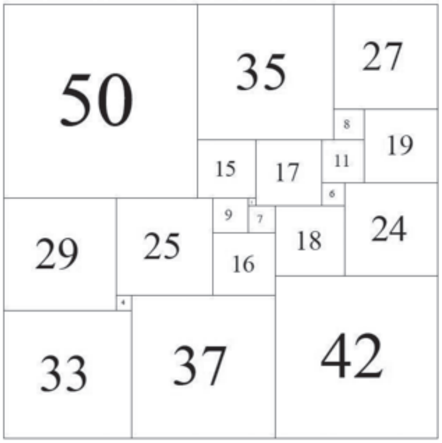


Figure 4
The smallest squared square is now the logo of the Trinity Mathematical Society (By kind permission of the Trinity Mathematical Society)

repeats every five letters, then the cipher is said to have a period of five. That means every fifth letter is encrypted using the same cipher. To work out the period, the dedicated code breaker might try looking for patterns, in this case writing the secret message in rows of five will reveal patterns that gives away the period. This is exactly the idea Tutte used to find a pattern in the Lorenz key.

After several unsuccessful attempts, Tutte took the key and wrote the first symbol of each letter in rows of forty-one – and spotted a pattern. This suggested that the first wheel in the machine had a period of forty-one. But the pattern was not perfect, which also suggested that the output involved another wheel that moved less regularly. This breakthrough was the first insight into the machine's structure.

After Tutte proved it could be done, the other members of the research station pitched in and within a few months had completely determined the structure of the machine. Soon after, replicas of the Lorenz were made for Bletchley personnel to decode messages; they were called Tunny machines. However, these replicas looked nothing like the real Lorenz machine which no one at Bletchley had ever seen. The reconstruction of Lorenz from one simple mistake remains one of the most remarkable achievements of the war.

Shortly after the end of the war, two Lorenz machines were captured in Italy and taken to Bletchley. Tiltman was asked to explain how they had broken into the system in the first place. Tiltman replied that they had initially used the twelve letter indicators at the beginning of the message. When it was pointed out that the captured machines had no letters on them, he replied, 'I can't help that, this is the first time I've seen it too.'

Breaking the Lorenz cipher

With the structure of the machine worked out, all the British codebreakers needed was a way to determine the pins on each wheel, a setting that changed every month. It was Alan Turing, taking a break from work on the Enigma, who devised a method to determine this setting.

Turing's idea was to deduce the pins by considering consecutive pairs of letters from messages that had been sent using the same settings. This method, laboriously performed by hand and requiring guesswork, was dubbed 'Turingery', but it was a method that few understood. Tutte later described Turingery as 'more artistic than mathematical'.

With the structure of the machine deduced, using Turingery to determine the pins and the wheel position that was obligingly transmitted at the beginning of each message, the team at Bletchley Park could read nearly every message sent from July to October 1942.

Then Lorenz operators changed their procedure. Now, instead of sending the wheel positions at start of the message, they were chosen from a code book, with only a number transmitted at the beginning. As a result the team at Bletchley Park needed a way to determine the wheel positions. Checking each wheel position was not possible. With twelve wheels of various periods, the number of possibilities was 16 million million million. Even if you could check a thousand per second it would still take 500 million years! It was Bill Tutte again who devised a method to work out the wheel positions.

In the same vein as Turingery, Tutte's procedure was to take consecutive pairs of letters of the code and consecutive pairs of letters generated by the Lorenz chi-wheels. He then added the first two symbols from each, using the usual teleprinter rules of addition. Tutte realized that if the two wheels were in the right position, the final result would be a dot 55 per cent of the time. This small clue could be used to determine the correct positions of the first two wheels.

The problem with Tutte's method was that process would have to be repeated for every letter of the message and every position of the first two wheels. A similar procedure would then have to be performed for all the other wheels. This method would be impossible to do by hand. When Tutte explained his idea to Max Newman, a leading Cambridge mathematician who had recently arrived at the research section, Newman came up with a way that the whole procedure could be performed electronically.

Newman's prototype machine was called Heath Robinson, after cartoonist William Heath Robinson's humorously elaborate machines. The pins' settings were punched on to one tape, while the code was punched on to another. These would then be read by the machine at high speed. Unfortunately, this could result in the tape tearing, breaking into fragments and flying off the machine. Despite being unreliable, Heath Robinson did prove that an electronic solution could work. What was needed was a better machine.

Tommy Flowers and Colossus

Colossus was the brainchild of Tommy Flowers, a brilliant engineer working for the General Post Office research branch at Dollis Hill, in north London. Flowers had joined the GPO in 1926 when he was twenty-one. He had been at Dollis Hill since 1930, developing telephone exchanges that used fast valves instead of mechanical relays.

It was Turing who recommended Flowers after working with him on a possible Enigma decryption machine. In February 1943 Flowers presented Newman with an idea for a fully electronic machine, containing one or two thousand valves that would generate the Lorenz key internally. Newman was sceptical of this proposal, believing a machine containing so many valves would be too unreliable. So, as Newman persevered with the Heath Robinsons, Flowers was left to pursue his idea with little support from Bletchley Park.

Flowers delivered his prototype Colossus on 18 January 1944. Generating the keys internally meant Colossus needed only one tape, containing the code. The machine read the tape optically, at an impressive 5,000 characters per second – meaning Colossus could complete Tutte's procedure in thirteen minutes. The machine attacked its first message on Saturday 5 February 1944, about which Flowers remarked in his diary, 'Colossus did its first job. Car broke down on the way home.'

As security was increased on the German side, pin settings on the Lorenz machine were now being changed daily rather than monthly. However, Flowers had deliberately built in more flexibility into his machine than was strictly necessary, allowing new codebreaking methods to be implemented as they were discovered. This flexibility is the reason why Colossus is sometimes considered to be the world's first programmable digital computer.

By the end of 1944 there were seven Colossus machines at Bletchley Park, and ten by the end of the war. These machines could be used to determine the pin settings as well as the wheel positions. Anything that could not be done by Colossus still relied on pencil-and-paper methods and language skills. All these methods together allowed the team at Bletchley Park to break those most important of German messages.

In that same year, 1944, decrypts revealed the German preparations for an Allied invasion of France, allowing the Allies to know as much about the German defences as the Germans themselves. Furthermore, not only were the Allies feeding the Germans misinformation, but breaking Lorenz meant they knew the Germans had fallen for it. By the end of the war, the team could break 90 per cent of messages sent by Lorenz.

After the war

When the war ended, Churchill ordered the Colossus machines to be destroyed and their existence classified. Unfortunately, this meant that the American ENIAC, or 'Electronic Numerical Integrator and Computer' known popularly as 'Giant Brain', which had been commissioned by the US army to calculate trajectories of artillery shells and which became operational in late 1945, received the credit as the world's first electronic digital computer.

Despite Churchill's orders, two Colossus machines were saved and taken away, first to the RAF station at Eastcote and later to Cheltenham, the home of the recently established Government Communications

Headquarters (GCHQ), and they remained there till around 1959. Immediately after the war, Russia used captured Lorenz machines to send their own secret messages – without realizing the British code breakers could break the code and read them.

John Tiltman continued to work as a senior codebreaker for GCHQ, as well as a liaison officer in the British embassy in Washington. Tiltman retired in 1954 at the age of sixty, but continued to work for the government service for another decade.

Tommy Flowers never received the recognition he deserved for the creation of Colossus. He received £1,000 as payment for his work, but this did not even cover his personal costs, and he shared most of it with the staff who helped him build Colossus. Flowers retired in 1969. A few years later he was given permission by the government to write about the technical aspects of his machine, but never about its purpose. In 1980 he was the first winner of the Martlesham Medal in recognition of his achievements in computing. And in 1993, at the age of eighty-seven, Flowers received a certificate from Hendon College, for completing a basic course in information processing on a personal computer.

In 1948 Bill Tutte moved to Canada and became a pioneer in graph theory, the mathematics of networks, which grew from a little-studied subject to its current highly active state. Tutte was made a fellow of the Royal Society in 1987. He never spoke about his work at Bletchley until shortly before his death in 2002.

Today there is a memorial to Bill Tutte in his home town of Newmarket, cleverly incorporating cryptic and subtle references to Bill Tutte and his achievement. It consists of metal strips with holes resembling the teleprinter tape used by Lorenz. On the ground a little further away is a squared square which is the ideal position to view the memorial. From this position, the holes of the teleprinter tape reveal a hidden portrait of Bill Tutte himself. It was created by acclaimed sculptor Harry Gray in September 2014.

Breaking Enigma may have saved Britain from defeat in the battle for the Atlantic in 1941, but breaking Lorenz provided information that Enigma could not. The combined efforts of all the codebreakers at Bletchley Park are believed to have shortened the war by two years, and in doing so saved countless lives.

10

Codebreaking after the Second World War

Markulf Kohlweiss, Nik Sultana and Tony Hoare

We all use code

Codebreaking was a vitally important activity during the Second World War since it provided some visibility into the enemy's intelligence and intentions. It involved a battle of wits that together with the battles on land and on sea changed the course of the whole war.

The scope of codebreaking has increased vastly since then. Most of us use code without thinking about it. Anyone who uses a mobile phone or a cash machine benefits from codemaking, or cryptography. Online commerce and Internet banking would not be possible without cryptography. Our phones and computers employ secret codes to communicate with each other.

Cryptography also affords us some private shade in the glaring public space of our connected world. It helps us shield our information and authenticate the identity of our communication partners. Cryptography helps protect us against criminals who want to steal information in order to steal identities and ultimately our money.

Along with the increase in scope of codebreaking, the power of computers, on which codebreaking relies, has grown vastly too. True to its name, the Colossus, which broke the infamous Lorenz code (see chapter 8), was colossal in size when compared to modern computers. But size is not an indication of power: a smartphone can do more computation in two minutes than the original Colossus did throughout its two-year life.[1]

The kind of codebreaking applied to the Enigma and Lorenz machines was somewhat different from that applied to Linear B (see chapter 3). The 'secrecy' of text in Linear B largely stemmed from the absence of knowledge of the syllabary in which it was written and the abbreviations used for common words. It was not the intention of the writers to hide their meaning. Furthermore, the content of the Linear B tablets was mundane, and in the same way most of our messages and documents are much less of a life-or-death matter than the wartime communications of the Second World War. Most of our daily communications are unremarkable, but taken together over time they draw a picture of our private lives. This detailed picture has commercial value: among other things it indicates what products and services we are likely to buy, what behaviour we are likely to engage in, whether we are living beyond our means, and what kind of advertising will appeal to us.

One of the contentious issues surrounding the modern-day application of cryptography is how we decide what is to be kept private, and what can be made available for other entities, such as those enforcing the law, to do their work without making us vulnerable to criminals or aggressive advertising. If all door locks are weakened to make it easier for the authorities to identify and intercept potential criminals, then those same locks can more easily be broken by criminals too.

In addition to having easy access to computer power, we also enjoy easy access to communication over the Internet. Morse code operators can communicate about a hundred characters per minute. Today's broadband Internet connections transfer more than 100 million characters per minute.[2] Furthermore, most data storage and computation is nowadays performed online on remote computers in data centres known colloquially as 'the cloud'. These digital storage systems, according to Roy Williams, a researcher at the California Institute of Technology (Caltech), would be sufficient to store every word ever uttered over the whole span of human history.

We face information-hungry adversaries in other nations and our own. They break into data centres to steal private information. They use ever faster, larger and more numerous machines, and might easily have the capability of storing all our encrypted and unencrypted communication. They include confidence tricksters and fraudsters, poison-pen tweeters and authoritarian regimes; they impersonate us, violate our privacy and siphon money from our bank accounts. They may also undermine our freedom and human rights. Code is part of the shield between them and us. How breakable is this code?

But what is 'code' and what does it mean to break it?

The word *cryptography* is derived from two ancient Greek words meaning hidden writing. It now covers all aspects of the deep theory and widespread practice of coding and decoding information. The original information is called *plain text*, and the output produced by encoding it is called *cipher text*. Translation is usually based on a secret key, which is presumed to be known only to the communicating parties. Discovery of the key indirectly by analysis is one of the ways of breaking the code. In this chapter we will use other words of Greek origin, referring to encoding as *encryption*, decoding using the key as *decryption* and breaking the code as *cryptanalysis*.

In popular usage, the word *code* has long been applied to any text that is not easily comprehensible. For example, a text in Morse code is less comprehensible to most people than the original text, though the letter-for-letter translations are widely published. Commercial codebooks of earlier times, which had the dual purpose of representing messages more compactly, were often just dictionaries, sorted differently in each direction for decryption and for encryption; they were kept secret to the company that wrote them. The Linear B text was originally called a code, simply because it was not understood; it was broken by some of the same linguistic methods (including guesswork) that are used for cryptanalysis.

There are other examples of the use of natural language as a secret code. French was spoken by the educated classes to discuss matters not suitable for the ears of their servants ('*pas devant les domestiques*'). And as late as the Second World War Navajo Indians were recruited to the US forces as radio operators to ensure the secrecy of local communication on the battlefields of the Pacific islands.

More recently, the word 'code' has been used for the text of a computer program, perhaps because programs can be extraordinarily opaque, often even to their authors. Early programs were written on coding sheets in machine code, so they could be stored directly in the memory of the computer for direct execution. The columns of the coding sheet held instructions, registers and addresses of operands in memory. Even now, programs written in a 'high-level' language (using idioms that are less machine-orientated, and more readable to humans) are called 'source code', translated by the computer itself into the 'object code' that it then executes directly.

This gives rise to a new meaning of the phrase 'breaking the code', otherwise known as hacking. Often, by exploiting some error in the program, the hacker gets the program to insert code written by the hacker into its own machine-code program held in the memory of the computer. In effect, the program is broken. Although it appears to work, it does not behave as intended by the programmer. Rather it behaves according to the intentions of the hacker, which are rarely benevolent. Nowadays, encrypted communications are often broken by hacking the programs that handle plain text and keys rather than by deriving the keys by cryptanalysis.

In the first two sections we assume that the program code of a cryptographic system follows its mathematical specification but we will get back to breaking program code in our section on code breaking as hacking.

'The enemy knows the system'

It is far easier to change the locks on the doors of your house than to build a new house with different locks. Similarly, it is far easier to change your computer password rather than buy a new computer, set a different password and transfer over all your files. The same idea holds for encryption: it is far easier to change the key than develop a new system. The development and validation of the encryption system itself is an intellectual task worthy of the genius of our most talented mathematicians, and although one might prefer to keep secret the operation of an encryption system, such details tend to leak over time especially if lots of people use them. This has been known for years: according to nineteenth-century Dutch cryptographer Auguste Kerckhoffs, 'A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.'

Claude Shannon, a contemporary of Alan Turing, put it more tersely: 'The enemy knows the system.' The *system*, but not the *key*. One can (and certainly should) try to retain good control over the encryption *key*, but it is often pointless to try to keep the entire encryption system secret. For example, a code can be something as simple as shifting the alphabet, so if we use a shift of three the word HI becomes KL. But we are not restricted to a shift of three, as there are twenty-six letters of the alphabet and therefore twenty-six possible shifts. So, in this example, shifting the alphabet is the system but there are twenty-six possible keys.

Shifting the alphabet can be easily broken by trying all the possible keys. We could make a code like this much harder by using more than one shift. For example, we could use a repeating pattern of four shifts (also known as a Vigenère cipher) as follows:

Shifts:	0	5	10	20	0	5	10	20	0	5	10	20	0	5	10
Message:	A	T	T	A	C	K	C	A	M	B	R	I	D	G	E
Code:	A	Y	D	U	C	P	M	U	M	G	B	C	D	L	O

This is a much stronger code; for example, double letters may not become double letters in the code. Such a key is said to have a period of four. There are 456,976 keys with a period of four. However, every fourth letter is encrypted using the same shift. This is a weakness that can be used by codebreakers to work out the original message. In general, keys with longer periods will produce stronger code.

Enigma worked on a similar system in that it used a different code for each letter of the message. In this case, Enigma was the system, and the Enigma settings were the keys. These settings included the choice of rotors and the plugboard settings, giving the huge number of 159 million million million Enigma settings. But the rotors turned after each letter, changing the code. This gave the key a long period of 16,900 before the pattern repeated. The statistics are mind-boggling.

The Enigma was used by some 40,000 operators at the height of the war. The settings changed every day, and operators in the same network needed to set their Enigma machines to the same configuration. These daily settings were written in key sheets, which were replaced every month. But in the case of Enigma, it was not so much the system that was the mystery; the challenge for the codebreakers was to identify the key the Germans were using on a given day.

Perfect security?

Are some keys better than others? Claude Shannon, known as the 'father of information theory', developed, among his many contributions to the science of cryptography, his mathematical proof that a cryptographic system can be perfectly secure. Imagine we again use different shifts for each letter of the message, but this time we create a sequence of random shifts with a period as long as the message itself. This pattern would not repeat, and trying every possible key for decryption will result in every possible message of that length. Shannon showed that the probability of making a decryption in a systematic way would be no different from applying guesswork. This is the definition of perfect security.

This scheme is secure, but it is difficult to make practical. It involves distributing a so-called 'one-time pad': a booklet or bundle of sheets containing a very long key, which can be used to encrypt text. Every time you want to encrypt a new piece of text, you start at the position in the key where you stopped last time. When a pad runs out, a new one is used. Pads should never be re-used.

Such pads were famously used, and sometimes re-used, by Soviet spies such as by the Cambridge spy ring in the UK and other spies targeting the Manhattan Project to develop the atomic bomb in the US. However, the difficulty of distributing fresh one-time pads to embassies led the Russians to re-use their one-time pads, and these 'two-time pads' betrayed them. The American Venona project, the counter-intelligence programme dating from the last years of the war into the 1980s, recorded encrypted messages, and in the case of pad re-use managed to decrypt a small but significant number of messages.

Hence an important factor for cryptanalysis is that if the key is shorter than the message, or it is re-used, then this gives the codebreakers clues to break the code.

Today, keys and messages are transmitted as ones and zeros. The size of a key is then measured in 'bits' – short for *binary digit*. So a 1-bit key consists of a single binary digit, whereas a 10-bit key consists of ten such digits, for example 1111101011. Every time you increase the key length by one, it doubles the number of keys. This is called exponential growth.

Legend has it that the inventor of chess used exponential growth to his advantage. When asked by a king how he would like to get paid for his invention, the inventor replied that he would like to receive one grain of wheat for the first tile, two for the second, four for the third and so on. The king gladly agreed, only to learn that he was ruined. The tally of 2^{64} grains is more than 16 million million million – more grains than has been produced in the entire history of wheat production! A chessboard representing the number of grains per tile is also a good visualization for the scale of today's computers and the amount of work it takes to recover a 64-bit key. This is feasible with today's hardware and within reach of organized political, commercial and criminal organizations.

The number of Enigma settings is comparable to eighty-bit keys, which is quite strong even by today's standards. The cryptographic weakness of the Enigma originated not from the number of settings, but from its mathematical structure (see chapter 7).

How many keys you need for secure encryption came into debate with the creation of the Data Encryption Standard (DES) which was published in 1975. In the early 1970s IBM had developed a cipher called Lucifer that was built as a practical approach to cryptography, using shorter keys. Lucifer formed the basis of DES. Following discussions with the US National Security Agency, IBM reduced its key size from 128 bits to 56.[3] This had the effect of halving the number of keys 72 times over. At the time the controversy was whether 56-bit keys were enough; the academic cryptographers Whitfield Diffie and Martin Hellman argued

Figure 1
'U-559' from which HMS 'Petard' sailors gathered the enigma codes
(Courtesy of German U-Boat Museum, Cuxhaven-Altenbruch, http://dubm.de)

that a special-purpose computer could be built to find DES keys by brute force. Such a machine was eventually built by the Electronic Frontier Foundation in the 1990s.

Back in the 1970s there were great hopes that DES would revolutionize cryptography. The key early uses of commercial cryptography were in banking, for the purpose of authenticating users at cash points (ATMs) and other bank terminals. Another application in the following decades was ecommerce, which relies on secure communication between unknown parties over the Internet.

Distributing keys to communication parties

The Germans employed about 40,000 Enigma operators. Every month all operators of an Enigma network would receive the same printed keying sheet with the rotor settings for each day.

This was an obvious weakness in the system. The compromise of one such book, as achieved with the capture of German submarine *U-559* by the HMS *Petard* (figure 1), at a great human cost off the coast of Egypt, would compromise a whole network for at least a month, and perhaps for more if the vessel had been equipped with key material for a longer voyage.

'Public-key' cryptography

The Germans could have strengthened their network by making keys specific to two communication partners. In that case, even if a key is compromised, communication protected by other keys is still secure. To

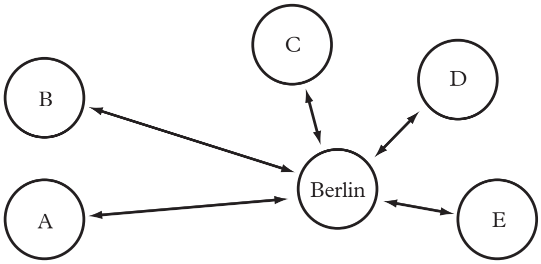


Figure 2
If A and B cannot communicate directly, and must communicate via Berlin despite being much closer to one another, then their communications will be slowed down
(Drawing by T. Richardson)

compromise all communication for a month, the codebreakers would have to steal almost 2 billion keys, a significantly harder task than stealing a single key.

But then every communication participant would need to store one key for every party it wants to communicate with. If every Enigma operator had to be able to talk to every other, then each would need their own unique book of 40,000 keys. This approach was just not viable with the technology of the time.

Alternatively, parties could relay messages over a central communication exchange, say Berlin, which alone knows the keys of all parties involved. But this has several problems: it slows down communication because it is not direct, it requires Berlin to be able to route messages for the whole network at all times and it thus creates a single point of failure: if Berlin cannot be reached (because of, for example, signal jamming or bombing) then the network cannot be used. So this approach was not viable either (figure 2).

In 1976, a few years after IBM's work on the DES, Whitfield Diffie and Martin Hellman, both computer scientists at Stanford University, discovered an ingenious solution to this problem. Together with another collaborator, Ralph Merkle, they conceived of a system in which the key used for decryption is distinct from the key used for encryption, and hard to compute from it. So the encryption key can be made public. They called this a 'public-key' cryptosystem. The decryption key is kept private by the person to whom messages are addressed, but the encryption key is shared with anybody who might want to send that person a message.

Diffie and Hellman's invention is based on number theory, which contains several problems that are easy to state, but hard to solve. For example, it is easy to multiply two large prime numbers, but factorizing the product (i.e. working out which two numbers you need to multiply to get the answer) of two large random primes is hard.

Let us use the analogy of a physical box that can be locked and opened using a physical key. In traditional cryptography you close and open the box with one and the same key. In public-key cryptography the public key and the private key turn in different directions. The public key turns anti-clockwise to lock the box, while the private key turns clockwise to open the box.[4] Alternatively, the public key operation consists of banging the door shut, engaging a spring bolt, which can only be withdrawn by inserting

Plain text	Cipher text
. . .	. . .
. . .	. . .
Canary	011010
Cat	010010
. . .	. . .
. . .	. . .
. . .	. . .

Cipher text	Plain text
. . .	. . .
010010	Cat
. . .	. . .
. . .	. . .
. . .	. . .
011010	Canary
. . .	. . .

Figure 3
The two parts of a codebook, left sorted by plain text, right by cipher text
(Drawing by T. Richardson)

and turning a private key that was not used at all in the locking operation.

Moving to the digital world, we can explain public-key encryption using codebooks (mentioned above). The first part of the codebook maps plain text to cipher text and corresponds to the public key. The second part contains the same list but sorted by code words, and it corresponds to the private key (figure 3). Without the second part decryption is much more difficult than encryption. Using modern computers, storing and sorting these lists is, of course, cheap so one can easily derive the private key from the public key, but imagine losing the decoding book on the battlefield and being left with only an encoding book. It allows you to encrypt quickly, but for decryption you might have to search many times through the whole book.

In December 1997 GCHQ revealed that its staff had discovered public-key cryptography before Diffie, Hellman and Merkle. Owing to an information-sharing arrangement, the secret history of 'non-secret encryption', as it was called within the agency, was well known to the closed community of readers of the internal NSA journal *CRYPTOLOG* (see further reading). GCHQ engineer James Ellis had thought of the concept (as Ralph Merkle had), after which their mathematicians Cliff Cocks and Malcolm Williams found efficient practical systems (as Diffie and Hellman had). However, only Diffie and Hellman had discovered the related concept of digital signatures. In a digital signature, the signer acts on a digital message using a private key in order to produce an authentication code that only the signer could have produced but that anyone in the world can verify using the signer's public key. This is critical to modern banking systems, to software updates (on the phone and computer) and to much else.

(Weakened) cryptography for everyone

How did cryptography leave the sphere of intelligence and warfare to become a tool for commerce and private communication?

Henry L. Stimson was an American statesman who oversaw the Manhattan Project. He was the pre-war Secretary of State in the US and later Secretary of War. In relation to wiretapping he famously said in the 1930s: 'Gentlemen do not read each other's mail.' This gentlemanly view of spying was trumped by the importance of codebreaking in the Second World War.

American and British intelligence agencies were rightfully proud of their contribution to the war effort. They had acquired a near monopoly on useful advanced cryptographic knowledge and naturally did everything in their power to preserve it. As a consequence they kept their successes secret, including public-key cryptography and cryptanalytic techniques.

In the 1970s the publication of the Data Encryption Standard and the seminal paper on public-key cryptosystems sparked off growing interest in cryptography in the academic and private sector. However, conflict soon arose with the secret world of intelligence. Academic cryptographers were questioning the reduction in key size from Lucifer's 128-bit keys to DES's 56-bit keys. In the secret world of intelligence agencies the *CRYPTOLOG* article on Diffie and Hellman's invention poked fun at Hellman's ability to attract press coverage and insinuates vested interests in discrediting the DES to create financial windfall for his own algorithms.

In the 1980s personal computers became a consumer product, and in the early 1990s sales started growing very rapidly. This was also an exciting time for commercial cryptography. By the 1990s, encryption was broadly deployed in global infrastructures for mobile phones and the Internet. We have seen that DES was weakened before standardization, how did weakened cryptography affect these new infrastructures?

Weakened cryptography on the Internet

Our communication with today's cloud data centres is encrypted using a protocol originally released in 1995 by Netscape, an early Internet browser vendor. One of the main contributors to this early deployment of cryptography on the Internet was Taher Elgamal, a student of Hellman who worked at Netscape. Netscape's protocol is now referred to as TLS for *transport layer security*. It uses public-key cryptography to exchange a key that is only shared between a web browser and server. This solves the key distribution problem for millions of web clients and servers and allows the establishment of an 'end-to-end' encrypted channel: in theory none of the relays between the two parties (such as the Internet Service Provider or ISP) should be able to decrypt the contents of your communication.

But this cryptography had to be made deliberately weak if it was to be exported for use outside the USA. American laws classified cryptographic software with keys longer than 40-bits as a munition. The motivation was to prevent the networks that were being rapidly designed and deployed in the 1990s from using strong cryptography as a default; the NSA knew that if networks adopted weak cryptography at the outset it would be difficult to improve them later, and these networks would likely remain open to surveillance.

Controls on other nations' cryptographic ability had a Second World War precedent. After the war, the Allied nations sold captured Enigma machines (which only they knew how to crack) to developing countries. This was deemed strategically important in the post-colonial and Cold War period, to obtain visibility into other countries' encrypted communications.

The weakened cryptography had unexpected, and unwanted, consequences. In the year 2000 the export restrictions on cryptography were partly lifted by the US, because of resistance from industry. There was fear that US companies would be at a disadvantage, if competition overseas could provide strong cryptography. However, the systems and software we use rely on established standards, and these standards evolve gradually, just as the NSA had anticipated. For better or worse, features from past versions of software become 'legacy', and are retained in new versions for compatibility. This is how somebody using an old computer and software can access today's Internet. The rationale here is that website owners are reluctant to say goodbye to even the 5 per cent of their users who are still using antiquated browsers. Thus modern web servers support suites of old cryptosystems, in case they need to communicate with an old web browser, and browsers similarly are often able to talk to old servers. This made users vulnerable to so-called 'downgrade attacks', where an attacker could manipulate network traffic to cause both a target server and a target browser to use an old and weak cryptosystem

Weakened cryptography on mobile phones

Another example of broadly deployed – but deliberately weakened – cryptography can be found in our mobile phones. In a 1982 article of *CRYPTOLOG* on new developments in telecommunications technology, the NSA anticipated the rise of mobile telephony. While the banking industry adopted DES, the global system for mobile communication (GSM) was developed in Europe and ended up using a French cipher design. Security researcher Ross Anderson reported,

> there was a terrific row between the NATO signal intelligence agencies in the mid-1980s over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the [Warsaw Pact]; but the other countries didn't feel this way, and the algorithm as now fielded is a French design.

GSM was deliberately designed to be no more secure than landline telephones, with weak encryption algorithms and a centralized key distribution system. Each mobile phone is uniquely identified by its International Mobile Subscriber Identity (IMSI) number and has its own authentication key stored in a chipcard to prevent cloning of mobile subscriptions. The phone identifies itself to a cell tower by stating its IMSI; the tower then contacts the phone's home network, and gets a challenge to send to the phone, a response that the phone will return to authenticate itself, and an encryption key for the connection. The encryption key and the response are calculated from the challenge using the authentication key in the chipcard.

This simple protocol has a number of weaknesses. For example, the phone cannot authenticate the cell tower, and so is vulnerable to wiretapping by a rogue tower; police forces use commercially sold devices referred to as 'IMSI catchers' to mimic towers. The encryption mode is also chosen by the tower, so an attacker can tell a mobile phone to use no encryption at all.

The GSM standard requires that users are informed about the lack of encryption, but few phones display this information.

The end-to-end revolution

Mobile phone networks and the Internet developed separately, but today the two have become highly intertwined. Mobile phones are increasingly the primary way to access the Internet for many people. This in turn enabled the development of new communication software whose popularity peaked after the disclosures by Edward Snowden in 2013, as people sought to shore up their online privacy.

Popular messaging software applications include Signal, WhatsApp, and Wire. On the surface, their messaging and voice features are similar to their GSM predecessors, except that as they run over data networks there are no call charges. People can therefore phone relatives overseas without paying huge bills. They can also create groups, a feature which phones did not easily support. As part of their programming, such messaging apps use Diffie and Hellman's public-key cryptography, and most of them continuously exchange keys that are only known by the phones of the communication participants. This is very different from GSM, where the encryption was much weaker, and only extended between the phone and the nearest cellphone tower. Moreover, keys are only kept for short periods of time. Such messaging apps are therefore not just much cheaper and more convenient to use; they are also much more secure against wiretapping and government surveillance generally.

Some governments now complain that they cannot enforce the law if their surveillance abilities are restricted. This reopened a 1990s debate on the extent to which governments should regulate the use of cryptography, and in particular whether it should systematically weaken cryptography, perhaps by introducing so-called 'back doors' for enforcement.

The 1990s debate involved two famous encryption systems. One was developed by the NSA and was only distributed in microchips, to keep their design secret. The other was created by Phil Zimmermann, a campaigner for nuclear disarmament, and distributed as a book to circumvent export restrictions.

The NSA system was known as the 'Clipper chip' (figure 4). It was initially meant for use in end-to-end encrypted phones. It relied on the exchange of an 80-bit key, for instance using public-key encryption. This key is then used to secure voice communication using a conventional encryption algorithm called Skipjack. The system came with a catch however. The Clipper chip contained additional keys, also known to the government, that were used to encrypt the key it used to encrypt plain text. This encrypted key was then attached to the cipher text. This enabled government organizations to listen in on the communication.

The other system was Pretty Good Privacy (PGP), named after a

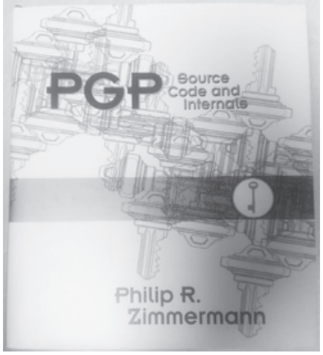


Figure 4 (left)
MYK-78, a 'Clipper chip'
(Travis Goodspeed, CC by 2.0)

Figure 5 (right)
Zimmermann's book containing PGP's source code
(Courtesy of Philip Zimmermann)

fictional grocery store from a radio show called *Ralph's Pretty Good Grocery*. Its inventor, Phil Zimmermann, uploaded it to Peacenet, an Internet service provider that specialized in grassroots political organizations, mainly in the peace movement. As this was accessible from outside the USA, PGP was soon available worldwide and Zimmermann became the target of criminal investigations for 'munitions export without a license'. Zimmermann challenged the export regulations in an imaginative way by publishing the PGP source code in a book (figure 5). The export of books is protected by the First Amendment of the US Bill of Rights.

PGP provides strong security, and evolved into a tool for encrypting emails that is popular among encryption enthusiasts. Fittingly, when writing this article we used a PGP encryption plug-in called Enigmail. The Clipper chip, on the other hand, was treated with suspicion by industry, and eventually the Clinton administration abandoned its attempts to force people to use cryptography with a built-in back door for the NSA and the FBI. The Snowden disclosures confirmed what was long suspected: intelligence services did not simply give up their attempt to gain access to keys but switched to more secretive ways. One of them is hacking.

Code breaking as hacking

Like the word 'code', the word 'hacking' has different interpretations. A popular one is the hijacking of a program to have it behave in a way that was not intended by its creators. For example, somebody might hack a website to paste in a political banner, or hack an ecommerce site to steal the details of its customers, or hack a bank's software to filch money from other people's accounts.

Hacking involves breaking program code by finding a way to change its behaviour to one's advantage. Most computer systems are so complex that they always contain weaknesses, like the loopholes in the law that tax accountants search for. These weaknesses can be found and exploited to control the computer system, and this is an effective way to sidestep the protection given by cryptography. Shannon insisted that *the enemy knows the system*, but the key question is: does the enemy know about the system's weaknesses as well? More practically, will he be able to find them and exploit them faster than you can find them and fix them?

This section describes two different kinds of hacking:

- The first exploits the fact that programs often interact with people, who are often the weakest link. In this way, a hacker breaks the code by deceiving the people who use it.
- The second exploits defects in the programs themselves.

After describing hacking we turn to ways to protect against hacking.

Human factors

Strong cryptography can be fatally weakened by how it is used. In theory, the Enigma relied on the use of a new key for each message. It was encrypted with the monthly key which was changed and placed at the start of the message, where each message could be at most 250 letters long. It was the responsibility of the message sender to invent a key for each message, but frequently senders re-used the same key, and that often enabled the Bletchley Park codebreakers to learn it. This is similar to the way in which people often re-use the same password to access different services online – stealing the password to one system grants an attacker access to others.

Hacking through human factors also includes manipulating people into compromising behaviour. An example from the Second World War is from the naval battle at Midway Island, which turned the fortunes in the Pacific theatre against Japan and in favour of the United States. The Japanese navy used a codebook, known as JN25, containing 90,000 words and phrases. Geographic locations in the JN25 code book were represented by a code group, and 'AF', the code for Midway, was at some critical moment unknown to the US Navy command. To learn the code for Midway, the American codebreakers sent a message to the island base over a secure underwater cable. The message instructed the base to send a message about the breakdown of their desalination plant via unencrypted radio such that it could be intercepted by the Japanese. In turn, the Japanese intercepted and forwarded the information about AFs desalinization plant encoded in JN25, thus revealing the code for Midway.

Bugs

It is often possible to hack programs without relying on the mistakes of their users, but by exploiting the mistakes of the program authors. 'Heartbleed' was an infamous mistake that exploited a feature designed to let a browser test whether the connection was 'live' by sending the server a 'heartbeat' signal that would be bounced back to prove that the server was still alive. This was an extension of TLS, the 'transport layer protocol' used to secure most web traffic.

The heartbeat message contains two pieces of information: a number picked by the sender, and an array of (arbitrary) characters whose total length is that number. For example, the sender's message could be (5, abcde) or (6, abcdef) – but not (5, abcdef) or (5, abcd). The receiver would then bounce this message back to the sender, to prove that it was alive.

Figure 5
Security company Codenomicon gave Heartbleed both a name and a logo, contributing to public awareness of the issue (Illustration by kind permission of Codenomicon)

The mistake in Heartbleed was simple: the receiver did not check that the content length was actually the same as the size of the content. The receiver would not only reply with the content from the sender, but would send additional data held in its memory at the locations where the message was stored. As TLS is an encryption protocol, the extra memory frequently contained secret keys and other private information such as passwords. The memory area used to store an array is called a 'buffer', and it is crucial that programs do not read or write outside these areas.

Computers simply follow their program and their behaviour can thus be much more self-destructive than that of any human operator. Through clever human engineering the Japanese navy operator was tricked into revealing an important codeword unintentionally. However, it is unlikely that a human would have handed out arbitrary data including private keys and user passwords in the same way as millions of Internet connected machines were happy to do for several years. And, it can get even worse.

Code injection

The first computing machines used by the Allies to break German ciphers were very specialized. Each performed a single cryptographic task. Alan Turing, Bill Tutte and their colleagues realized, however, that in order to break the most difficult codes they needed to ask a series of questions of these machines, with each question informing the next. In other words, they needed the computers to be more easily programmable.

The Colossus was the first programmable computer that could be used for a variety of tasks that had not been anticipated when it was first designed. This reprogramming still needed to be done by hand, by adjusting switches and plugs, rather than by editing a stored program. Having a 'stored program' means that the computer receives two kinds of input: one kind consists of programs, and the other kind consists of data – the input that is processed by programs.

Stored programs are today simply referred to as software. Software is what makes today's computers so powerful and flexible. This power can be abused though: what if, instead of regular program input, we were to maliciously feed another program as input? It can be very difficult for a computer to keep track of what input to treat as data, and what input to treat as a program. This forms the basis of so-called 'buffer overflow' attacks described above that inject programs into existing programs, to take over the computer.

Mitigation

Designing secure and dependable systems is still an area of active research. Programmers are taught how to avoid common pitfalls that make their code easier to break. There are tools and techniques that make their job easier and the job of their attacker more difficult.

One such tool, called 'address space layout randomization', shuffles the memory locations of running programs, making it harder for an attacker to obtain predictable results when injecting code.

Another option consists of using programming languages that carry out stricter checks on programs, to ensure the absence of broad classes of bugs.

An important programming technique was first explored by Turing, and involves the use of 'assertions' in the program code (see Morris and Jones, 1984). Assertions consist of logical formulas that must hold on every execution of the program. Sometimes it is possible to deduce these formulas to hold without actually running the program, that is, one proves a mathematical theorem about the program.

This is not always possible (as a consequence of Turing's 'Halting Problem' argument, which identified the problem of whether one can know if a computer program will finish its task or continue to run forever), and writing programs in a style that facilitates proofs is subject to ongoing research. As a safety measure, these formulas can also be checked during every execution of the program, and if an assertion fails then the program is shut down, to reduce the opportunity of an attacker to exploit it.

Today, the increased power of modern computers, and the development of powerful proving techniques, makes theorems about complex and error-prone protocols such as TLS possible, as was the original idea of Turing. This is a monumental task and fittingly the project at Microsoft Research that is attempting it is called Everest.

The moral dimension of codebreaking and groundbreaking

The DĀMOS database of Mycenaean at Oslo stores the annotated searchable corpus of excavated Linear B tablets. According to researcher Federico Aurora the known corpus of Linear B consists of about 70,000 signs (see chapter 5). [5] Much of this data contains inventories of goods, land, workers, personnel and registrations of their movement in and out of the palaces. According to *Wired* magazine, the Utah data centre of the NSA stores exabytes, about 2^{60} or 1 million million million bytes, of our Internet communication. It stores 'the complete contents of private emails, cell phone calls, and Internet searches, as well as all types of personal data trails – parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter"'. The clay tablets of Mycenaean palace cultures and the database tables of modern data centres have something in common: they both are record-keeping systems about everyday life maintained by powerful, centralized bureaucracies.

The technical advances made during the Second World War, such as programmable computers and the atomic bomb, had a lasting impact on our world. Mathematicians, scientists and engineers are largely responsible for technical advances, but to what extent should they be morally concerned? It is an uncomfortable responsibility, since the training of scientists, mathematicians and engineers focuses much more on deep, puzzling, technical problems rather than human and societal ones; policy and its consequences are seen as somebody else's problem. Moreover, the big picture keeps changing: sometimes the down side of an invention only appears long after it was developed and policies were formed about it.

Cryptographer Phil Rogaway draws parallels between the responsibility of the nuclear scientist and the computer scientist. A concern for socio-political problems touching technology is visible in Diffie's and Hellman's criticism of DES's key length, but academic cryptography in the 1980s and early 1990s was not always that practically minded. An NSA trip report published in *CRYPTOLOG* about an academic conference in 1992, states: 'There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. I really don't see how things could have been better for our purposes.'[6] This changed once the Clinton administration launched the Clipper chip, and a number of cryptographers engaged in public advocacy for privacy and human rights. Does cryptography have an important emancipatory role, as well as protective one?

In his memoir *Wind, Sand and Stars* Antoine de Saint-Exupéry describes his experience of extreme solitude as an airmail pilot alone over Argentina. He notices a few flickering lights on an almost empty plain that 'twinkled here and there, alone like stars'. Since the 1930s, when these words were written, technological advances have changed our world from a place in which we are private by default to a world in which we are connected by default. The value of our data and the availability of cheap storage also mean that we are recorded by default. We still do not fully understand the consequences that this can have on people and on our society. Today, to be truly alone we must be in full control of our devices and their sensors; to communicate privately we have to use encryption.

Program and encryption codes have advanced a lot since the Second World War, and become prevalent. But we now find that breaking code in peacetime can be just as consequential as breaking code in wartime.

Epilogue

James Clackson

John Chadwick noted in his book *The Decipherment of Linear B* (1958) that 'There is an obvious resemblance between an unreadable script and a secret code; similar methods can be employed to break both.' (cited by Burman, chapter 6). This publication and the accompanying exhibition explore the connection, and show the links between decipherment and decryption. Undeciphered ancient scripts and encoded messages encase the underlying texts in a seemingly impenetrable shell that can only be cracked through human insight, imagination, repeated trial and error, and – sometimes – lucky guesses. The articles in this volume have explored the methods used for the two most famous codebreaking achievements of the twentieth century: the reading of the Linear B archival records from second millennium BC Greece and the decryption of the Enigma and other codes of the Axis powers in the Second World War.

As the exhibition and the book have shown, however, the similarity between the solving of these two puzzles is not limited to a resemblance of methods employed. The two events are closely linked in time, place and people. The decipherment of Linear B came less than a decade after the decryption work at Bletchley Park, where John Chadwick himself was employed in the war, and he was only one of several of the codebreaking classicists who later turned their attention to Linear B. Indeed, it is especially appropriate that this exhibition has been held in Cambridge, since many of the mathematicians, classicists and others recruited to work at Bletchley Park were academics employed in or educated at Cambridge University and Cambridge has been closely associated with research into the archaeology and epigraphy of Minoan and Mycenaean Greece for over a century. Some of the most important documentary evidence for the decryption of the Enigma code and the decipherment of Linear B are kept in Cambridge: the Archive Centre at Kings College, Cambridge, holds the papers of Alan Turing and the Faculty of Classics in Cambridge houses both the A. J. B. Wace Archive of Mycenaean Archaeology and the Chadwick Archive, which includes the correspondence between Ventris and Chadwick.

Among these many points of contact, perhaps the most notable similarity between the two great codebreaking exploits of the last hundred years lies in the characters of Alan Turing and Michael Ventris. Both men shared aspects of personality and working habits that allow them to be slotted into a convenient Hollywood model of the maverick outsider, untiring in their pursuit of truth. Both died young in tragic circumstances, Turing in 1954 and Ventris in 1956. In the popular imagination Ventris and Turing have become for the twentieth century what Jean-François Champollion, decipherer of Egyptian hieroglyphs, was for the nineteenth (it is perhaps significant that the modern three code-breaking events discussed in detail Simon Singh's *The Code Book* (1999) are Egyptian hieroglyphs, Linear B and Enigma). These codebreakers have come to be seen in the same light as romantic heroes who overcome apparently insuperable odds to win the day, although it is through their mental attributes rather than physical prowess that they manage to solve the insoluble. The hero-decipherer is a modern type of hero – earlier writers on codes and cyphers, such as Francis Bacon, saw the art of encryption as that which required 'great pains and a good wit' (*Of the Advancement and Proficience of Learning*, translated Gilbert Watts, 1674, p. 175). The famous names in the history of ciphers from before the modern period are those who devised codes, from Julius Caesar to Blaise de Vigenère, rather than those who broke them.

The romantic hero model perhaps helps to explain why these codebreaking achievements have found fame in a way that others have not done. None of the other decipherments of ancient scripts of the last two hundred years has caught the public's attention in the same way that hieroglyphs or Linear B have, and none of the other decryptions are as widely known as Enigma. Most other decipherments have proceeded in a more piecemeal fashion, with no single identifiable hero genius in the mould of Champollion, Ventris or Turing. The decipherment of the Mesoamerican writing systems used by the Mayan civilization, for example (memorably written up by Micheal D. Coe in his 1992 book *Breaking the Maya Code*), was achieved through successive insights by a number of different scholars: Yuri Knosorov, Tatiana Proskouriakoff, Linda Schiele and others, including Michael Coe himself. The Mayan decipherment, moreover, remains an ongoing project. Even now, many Mayan sign groups and inscriptions are still obscure, with a recent estimate that 40 per cent of the estimated 800 signs are still undeciphered (http://mayawoerterbuch.de/milestone-report-2014-2016/ accessed July 2017).

The material gathered in this book reminds us to be a little mistrustful of the paradigm of the codebreaker as a lone (male) genius hero. As the articles here show, the achievements of the Linear B and Enigma codebreakers are less monolithic than would appear from the Hollywood version. Ventris and Turing both justly merit the overused epithet of genius, but their successes were underpinned by the work and support of many others. Genius flourishes in an environment of interchange of ideas, co-operation and trust, and it is appropriate that in this volume we are reminded of some the other figures who are too often written out of the story, including Alice E. Kober (whose pioneering work on Linear B was crucial to Ventris's success), and Emmett L. Bennett; and the Polish mathematicians who were the first to 'break' Enigma, Marian Rejewski, Henryk Zygalski and Jerzy Różycki. It is good also to preserve the memory of some of the other stunning achievements of cryptanalists working at Bletchley Park, including Bill Tutte's success with the Lorenz code.

The book has also shown some of the divergences between decipherment and decryption. Ancient scripts are in origin intended to be learnable and readable by anyone who has undergone scribal training, whereas encoded texts have been deliberately manipulated to conceal their underlying message. Encryption attempts to make sure that there are no readily identifiable repeated patterns of the type which the decipherment of ancient script relies upon. In the case of Linear B, it was repeated sequences known as Kober's triplets that allowed Ventris to construct the essential grids relating signs to consonant and vowel values for specific signs. On the other hand, the cryptanalyst is given the advantage that the language in which an encoded message has been written can normally be assumed at the start of the enterprise, whereas most decipherers are faced with cracking both a script and a new language (or at least a different dialect from anything currently known).

The underlying differences between decipherments and decryption have profound consequences for the current and future state of code-breaking. Encryption has now moved far beyond the ciphers and letter substitutions that lay behind earlier codes – even the Enigma and Lorenz codes were in effect sophisticated means of finding letter substitutions. Encryption has also become pervasive in modern life: codes are no longer the preserve of secretaries and clerks in the courts of princes, as they were in Francis Bacon's day, or limited to governments and the military. Most individuals rely on encryption on a daily basis for everything from financial transactions to text messages. Modern encryption systems make heavy use of the enormous processing power of computers and supercomputers, which can perform calculations in a second that would take an individual many lifetimes. As Markulf Kohlweiss, Nik Sultana and Tony Hoare explain in chapter 10, the successful cryptanalyst of today is more prone to be branded a computer hacker than a hero, and in the twenty-first century it is once more encryption rather than decryption which is seen as the work of genius. The most famous living cryptanalysis of today is probably Satoshi Nakamoto, the inventor of bitcoin. Satoshi Nakamoto is, appropriately, a cipher, whose real identity and whereabouts are unknown, although of a net financial worth estimated to be well over a billion dollars.

The application of the latest technological developments to undeciphered ancient scripts and languages is sometimes trailed as offering new possibilities for decipherment. For example, in October 2012 the Oxford assyriologist Jacob Dahl told the BBC that a new initiative to digitize high quality three-dimensional images of tablets with the script known as Proto-Elamite was a breakthrough that could lead to its decipherment within a couple of years (http://www.bbc.com/news/business-19964786 accessed July 2017). Federico Aurora, in chapter 5 of this volume, gives indications of some of the digitization initiatives that have taken place recently for the Aegean scripts. But both for Proto-Elamite and the Aegean scripts, digitization only serves to enhance the material available for other scholars, and the promise offered by the new technology has not so far been fulfilled. Even the computational tools described by Aurora for decipherment are designed to 'encode some of the linguistic intuitions' of human researchers, rather than come up with the intuitions. There is still a need for human agency in the ongoing work of decipherment of Linear A, proto-Elamite and the half-dozen or so other writing systems that have evaded elucidation to date. Making headway in the interpretation of these codes relies upon a combination of linguistic and cultural knowledge and a flexibility of mind which it has not yet been possible to programme into a computer. Even so, the likelihood is that we will not see another Jean-François Champollion or Michael Ventris crack any of the remaining undeciphered scripts, but that decipherment, if it comes at all, will be of the piecemeal, team effort sort which has worked for Mayan hieroglyphs. Indeed, for the Linear A and Cypro-Minoan writing systems (discussed by Pippa Steele in chapter 4), work currently taking place in Cambridge and elsewhere is making gradual progress towards understanding the nature of the script and interpretation. An increasing number of signs and sign-groups on the Linear A tablets can be read with some confidence, even though the exact nature of the underlying language remains unknown. The shell of obscurity around Linear A and Cypro-Minoan will probably not be 'cracked' in the same way that Ventris can be said to have cracked Linear B in June 1952, but painstakingly worn down through collaborative research.

In conclusion, it seems as if the 'heroic age' of decryption and decipherment has now passed. For cryptanalysis, the methods of computer science which Turing inaugurated have led to the rise of the supercomputer; cryptanalysis is no longer in the business of decoding, but of computer programming. Over the last two hundred years, scholars have made sense of the great majority of undeciphered scripts from the ancient world with records in sufficient numbers to observe repeating patterns or in a linguistic variety which can be related to previously known languages. It is now possible to read texts not just in Egyptian and Mayan hieroglyphs, but also in hieroglyphic Luwian; in cuneiform recording Akkadian, Elamite, Hittite, Hurrian, Luwian and Sumerian; in the Linear B and Cypriot syllabaries; in alphabetic or quasi-alphabetic writing systems of Bactrian, Carian, Etruscan, Lycian, Nabatean, Oscan, Old Persian, Old South Arabian, Old Turkish, Phoenician, Sogdian, South Picene, Ugaritic, Umbrian and the different languages using the Kharosthi script – and this list is by no means comprehensive! The number of remaining ancient or medieval scripts which have not been deciphered is small, and for none does an extensive corpus of texts survive. Barring new discoveries, the opportunities for another stunning decipherment are accordingly extremely limited. The achievements of the codebreakers in mid-twentieth century Britain are consequently likely to remain as the most notable of all time. This exhibition and book is a fitting tribute not just to the genius of Turing and Ventris, but to all the other contributors and collaborators, not to mention the intellectual climate, that made these achievements possible.

Appendix

List of Objects

Colour plates lie between pages 66-7 and 82-3

The Decipherment of Linear B

1 *Silver coin of Knossos showing Minotaur on one side and labyrinth on the other (figure 1 in chapter 1, p. 2).* Crete was known through stories as the birthplace of Zeus, home of the labyrinth and of the half-man, half-bull (the Minotaur). This coin from Knossos illustrates the engagement of the Cretans with their glorified past. The myths drew antiquarians to the island who started exploring its art and archaeology more systematically from the nineteenth century onwards. No one, however, could guess that writing might have existed on the island or on pre-classical Greece as a whole.
Silver, about 500 BC, 2.3 cm
CM.MC.7050, McClean Collection, Fitzwilliam Museum, University of Cambridge

2 *Four-sided seal inscribed in Cretan Hieroglyphic purchased by Arthur Evans at Palaikastro, east Crete, in 1894 (plate 1).* It was a similar stone that first inspired Evans to search for clues for pre-alphabetic writing in the Aegean. On the engraved sides, he saw signs of early writing, not just images. In Crete these stones were locally known as *galopetres* – charms which, according to popular Cretan folklore, ensured the flow of milk to lactating mothers. Evans collected hundreds of these during his trips and was able by 1895 to prove the existence of at least two pre-alphabetic scripts: Cretan Hieroglyphic and Linear A. Eager to date these documents and situate them in their historical and cultural context, he decided to excavate Knossos – a place with a long mythical history and with visible ruins from earlier excavations suggesting the existence of an important pre-classical settlement.
Jasper, around 1850–1700 BC, 1.7 x 0.5 cm
AN1896-1908/AE.1774, Ashmolean Museum, University of Oxford

3 *Seal showing a butterfly, bought by Arthur Evans at Makryteichos near Knossos in 1894 (plate 2 and figure 1 overleaf).* Evans bought this gem, along with a few other objects, from a schoolmaster from the village next to the ruins at Knossos. He was not the first to notice the importance

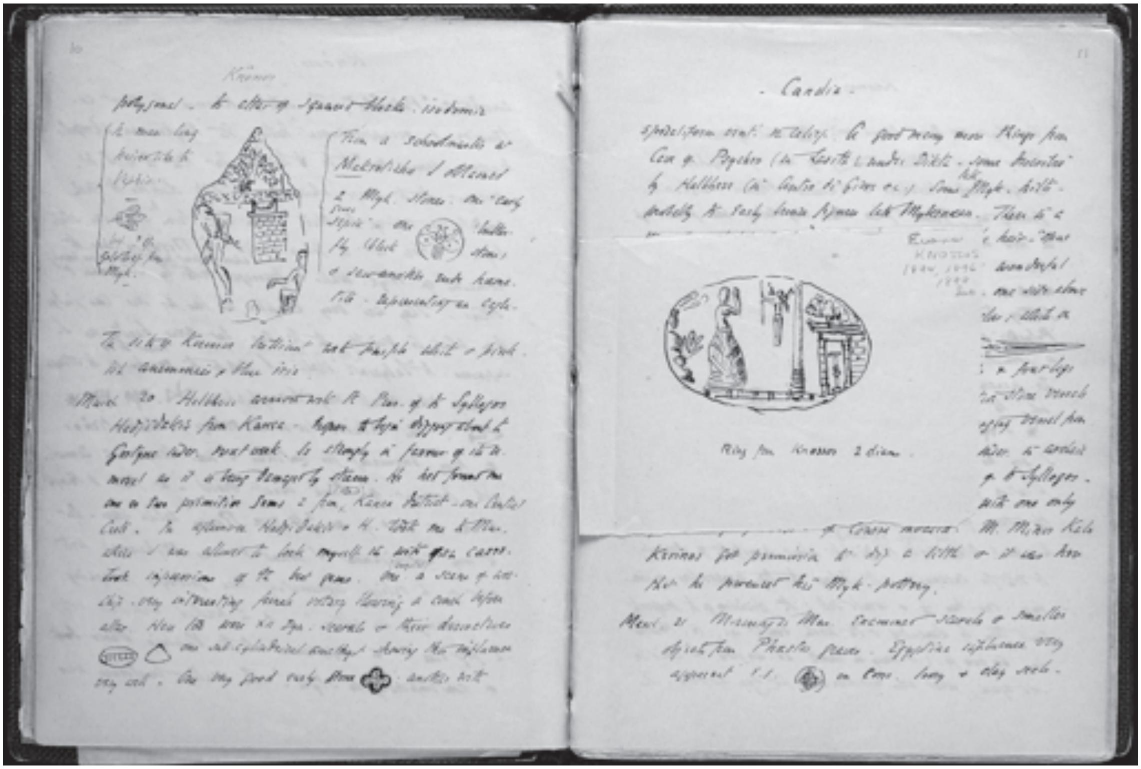
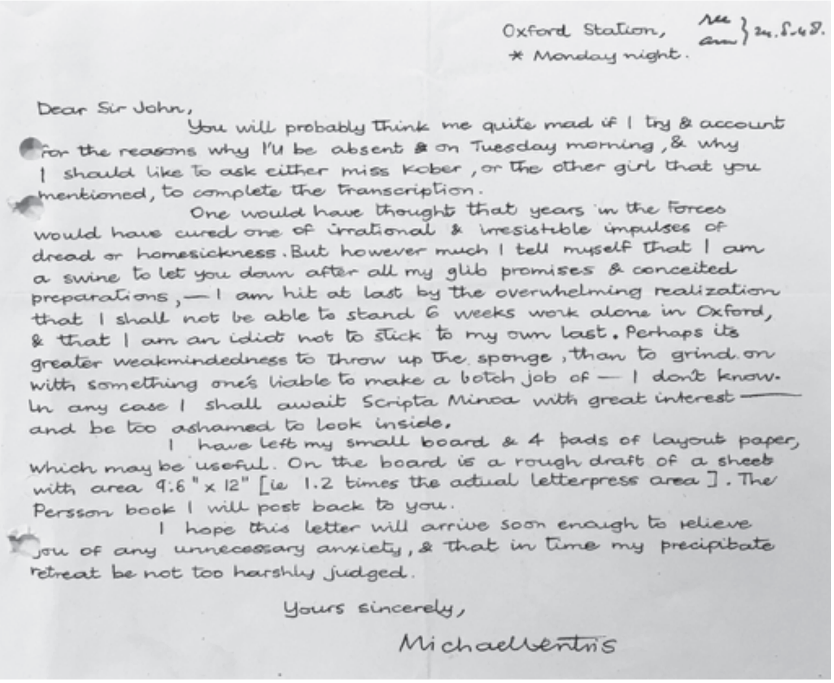

- Candia -
Ring from Knossos 2 diam.

Figure 1
Two pages from Arthur Evans's 1894 Cretan travel diary. Entries 3 and 4 are recorded on either side with accompanying drawings. (Courtesy of the Ashmolean Museum, University of Oxford)

of the ruins there, which had been partially uncovered in the 1870s by a Cretan antiquarian named Minos Kalokairinos. Schliemann had also tried to excavate Knossos but failed. Evans managed to purchase the land where the ruins stand and to conduct the first systematic excavations, with interruptions, from 1900 to 1931.
Serpentine, about 1600–1450 BC*, diameter 1.4 cm*
AE1938.968, Ashmolean Museum, University of Oxford

4 *Gold signet ring with a 'scene of worship', said to come from Knossos, bought by Arthur Evans at Herakleion in 1894 (plate 3 and figure 1).* Following the gold-rich discoveries of Heinrich Schliemann at Mycenae in mainland Greece in 1876, Evans was convinced that the origins of this glorious pre-classical civilization must be sought in Crete, and that writing existed in that part of the world long before the alphabet made its first appearance. This ring was one of the first objects that Evans purchased as soon as he set foot on Crete. An avid collector and traveller, he made several trips to the island, gaining valuable knowledge of its history, art and archaeology.
Gold, about 1600–1450 BC*. 2.2 x 1.2 cm (bezel)*
AN1938.1127, Ashmolean Museum, University of Oxford

5 *Michael Ventris quits the 'Scripta Minora' project. Letter from Michael Ventris to John Myres (received 24 August 1948, figure 2).* John Myres invited



Oxford Station, Mon am } 24.8.48.
* Monday night.

Dear Sir John,

You will probably think me quite mad if I try & account for the reasons why I'll be absent on Tuesday morning, & why I should like to ask either miss Kober, or the other girl that you mentioned, to complete the transcription.

One would have thought that years in the Forces would have cured one of irrational & irresistible impulses of dread or homesickness. But however much I tell myself that I am a swine to let you down after all my glib promises & conceited preparations, — I am hit at last by the overwhelming realization that I shall not be able to stand 6 weeks work alone in Oxford, & that I am an idiot not to stick to my own last. Perhaps its greater weakmindedness to throw up the sponge, than to grind on with something one's liable to make a botch job of — I don't know. In any case I shall await Scripta Minoa with great interest — and be too ashamed to look inside.

I have left my small board & 4 pads of layout paper, which may be useful. On the board is a rough draft of a sheet with area 9.6" x 12" [ie 1.2 times the actual letterpress area]. The Persson book I will post back to you.

I hope this letter will arrive soon enough to relieve you of any unnecessary anxiety, & that in time my precipitate retreat be not too harshly judged.

Yours sincerely,

Michael Ventris

Figure 2
The letter from Michael Ventris to John Myres announcing that he wished to quit the 'Scripta Minoa' project.
(Courtesy of the Ashmolean Museum, University of Oxford)

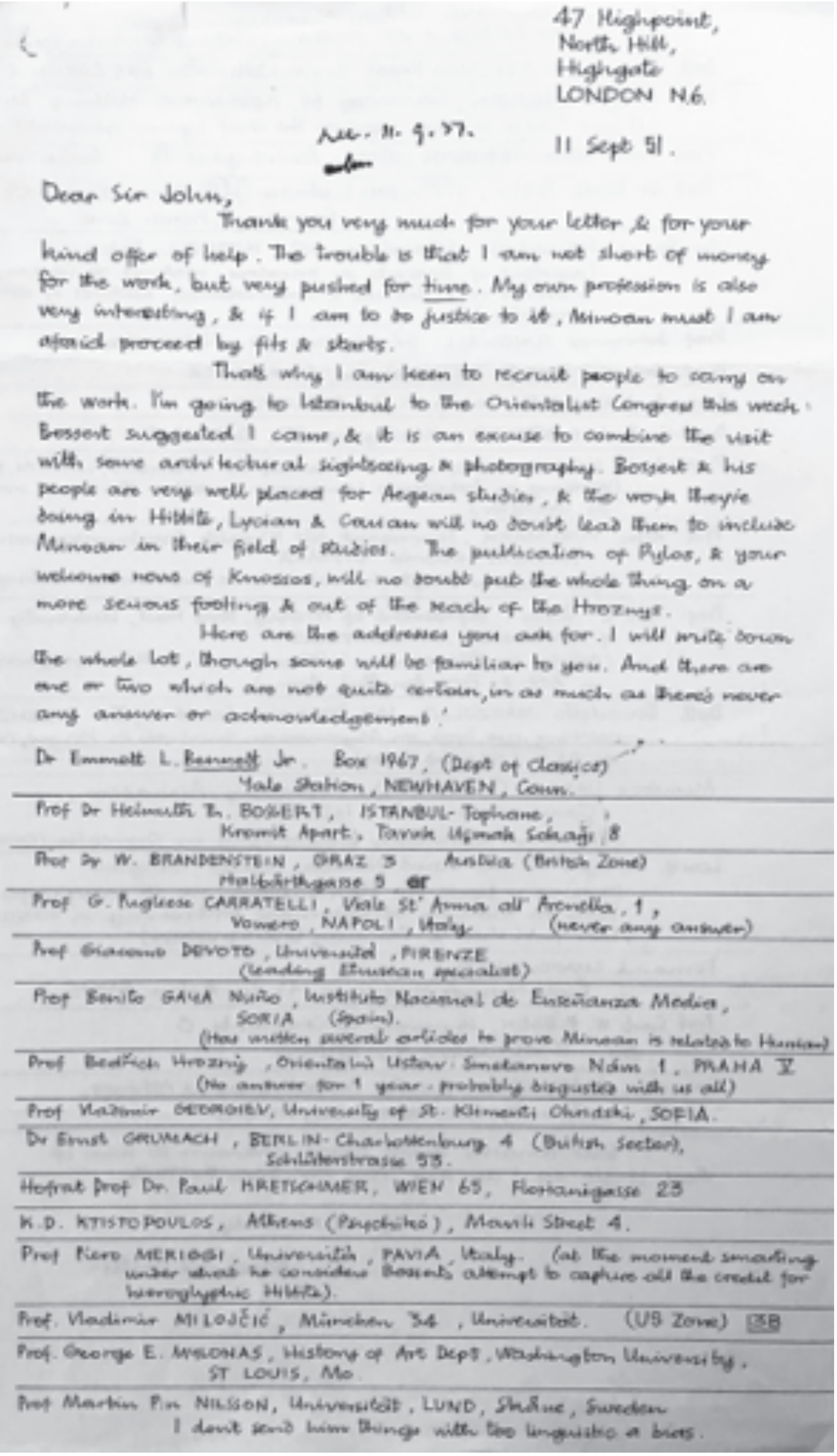
Michael Ventris to help him with the publication of *Scripta Minoa*, the Linear B documents from Knossos. In this letter Ventris pulled out at the last minute, before meeting Alice Kober, Myres's main collaborator at the time. The path to decipherment had for Ventris many ups and downs but his sheer determination to crack the code made him return to his Linear B pursuits not long after this letter was written.
Paper and ink (handwritten), length 16.5 cm, width 21 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

6 *Mid-Century Report, 1950 (not illustrated).* This booklet contains a set of questions circulated by Michael Ventris late in 1949 to all scholars working on Linear B in an attempt to restart efforts for its decipherment and get the most up-to-date knowledge of where things stood. Alice Kober was one of the few who declined to reply. She thought it was a waste of time, most likely because of its focus on the language of Linear B which she considered unhelpful speculation. Although the Mid-Century Report was meant to be Ventris's last small contribution to the problem, he soon gave up his main job (as an architect) to work full time on Linear B.
Bound booklet, typed, length 32.9 cm, width 20.4 cm (when closed)
Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge

7 *Letter from Michael Ventris to John Myres (11 September 1951, figure 3).* In this letter Ventris produces a list of all the people with whom he is in contact. Like Myres, Ventris was in favour of collaborative working as he believed that sharing information and exchanging notes could speed up the

Figure 3 People working on Linear B (Courtesy of the Ashmolean Museum, University of Oxford)

Figure 4 (opposite) Letter from Alice Kober to John Myres, 18 February 1950 (Courtesy of the Ashmolean Museum, University of Oxford)



47 Highpoint,
North Hill,
Highgate
LONDON N.6.

Ans. 11. 9. 57.

11 Sept 51.

Dear Sir John,

Thank you very much for your letter & for your kind offer of help. The trouble is that I am not short of money for the work, but very pushed for time. My own profession is also very interesting, & if I am to do justice to it, Minoan must I am afraid proceed by fits & starts.

That's why I am keen to recruit people to carry on the work. I'm going to Istanbul to the Orientalist Congress this week. Bossert suggested I came, & it is an excuse to combine the visit with some architectural sightseeing & photography. Bossert & his people are very well placed for Aegean studies, & the work they're doing in Hittite, Lycian & Carian will no doubt lead them to include Minoan in their field of studies. The publication of Pylos, & your welcome news of Knossos, will no doubt put the whole thing on a more serious footing & out of the reach of the Hroznys.

Here are the addresses you ask for. I will write down the whole lot, though some will be familiar to you. And there are one or two which are not quite certain, in as much as there's never any answer or acknowledgement.

Dr Emmett L. Bennett Jr. Box 1967, (Dept of Classics)
Yale Station, NEWHAVEN, Conn.

Prof Dr Helmuth Th. BOSSERT, ISTANBUL-Tophane,
Kromit Apart., Tavuk Uçmak Sokaği 8

Prof Dr W. BRANDENSTEIN, GRAZ 3 Austria (British Zone)
Halbärthgasse 5 or

Prof G. Pugliese CARRATELLI, Viale St' Anna all' Arenella, 1,
Vomero, NAPOLI, Italy. (never any answer)

Prof Giacomo DEVOTO, Università, FIRENZE
(leading Etruscan specialist)

Prof Benito GAYA Nuño, Instituto Nacional de Enseñanza Media,
SORIA (Spain).
(Has written several articles to prove Minoan is related to Iberian)

Prof Bedřich Hrozný, Orientalni Ustav Smetanovo Nám 1, PRAHA I
(No answer for 1 year - probably disgusted with us all)

Prof Vladimir GEORGIEV, University of St. Kliment Ohridski, SOFIA.

Dr Ernst GRUMACH, BERLIN-Charlottenburg 4 (British Sector),
Schlüterstrasse 53.

Hofrat Prof Dr. Paul KRETSCHMER, WIEN 65, Florianigasse 23

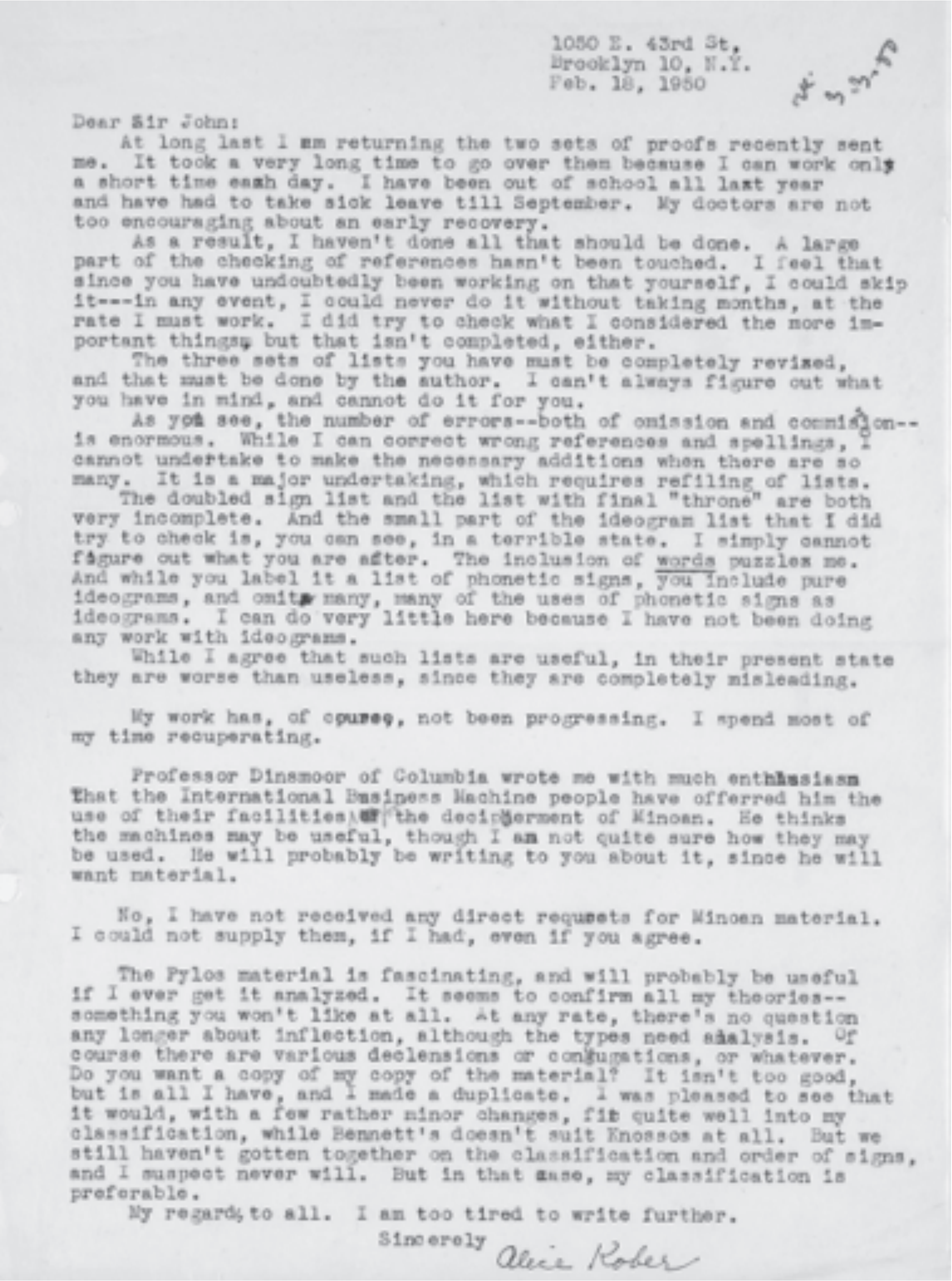
K.D. KTISTOPOULOS, Athens (Psychiko), Mousi Street 4.

Prof Piero MERIGGI, Università, PAVIA, Italy. (at the moment smarting under what he considers Bossert's attempt to capture all the credit for hieroglyphic Hittite).

Prof. Vladimir MILOJČIĆ, München 34, Universität. (US Zone) 13B

Prof. George E. MYLONAS, History of Art Dept, Washington University,
ST LOUIS, Mo.

Prof Martin P:n NILSSON, Universitet, LUND, Skåne, Sweden
I don't send him things with the linguistic or bits.



1050 E. 43rd St,
Brooklyn 10, N.Y.
Feb. 18, 1950

[illegible]

Dear Sir John:

At long last I am returning the two sets of proofs recently sent me. It took a very long time to go over them because I can work only a short time each day. I have been out of school all last year and have had to take sick leave till September. My doctors are not too encouraging about an early recovery.

As a result, I haven't done all that should be done. A large part of the checking of references hasn't been touched. I feel that since you have undoubtedly been working on that yourself, I could skip it---in any event, I could never do it without taking months, at the rate I must work. I did try to check what I considered the more important things, but that isn't completed, either.

The three sets of lists you have must be completely revised, and that must be done by the author. I can't always figure out what you have in mind, and cannot do it for you.

As you see, the number of errors--both of omission and commission--is enormous. While I can correct wrong references and spellings, I cannot undertake to make the necessary additions when there are so many. It is a major undertaking, which requires refiling of lists.

The doubled sign list and the list with final "throne" are both very incomplete. And the small part of the ideogram list that I did try to check is, you can see, in a terrible state. I simply cannot figure out what you are after. The inclusion of words puzzles me. And while you label it a list of phonetic signs, you include pure ideograms, and omits many, many of the uses of phonetic signs as ideograms. I can do very little here because I have not been doing any work with ideograms.

While I agree that such lists are useful, in their present state they are worse than useless, since they are completely misleading.

My work has, of course, not been progressing. I spend most of my time recuperating.

Professor Dinsmoor of Columbia wrote me with much enthusiasm That the International Business Machine people have offerred him the use of their facilities for the decipherment of Minoan. He thinks the machines may be useful, though I am not quite sure how they may be used. He will probably be writing to you about it, since he will want material.

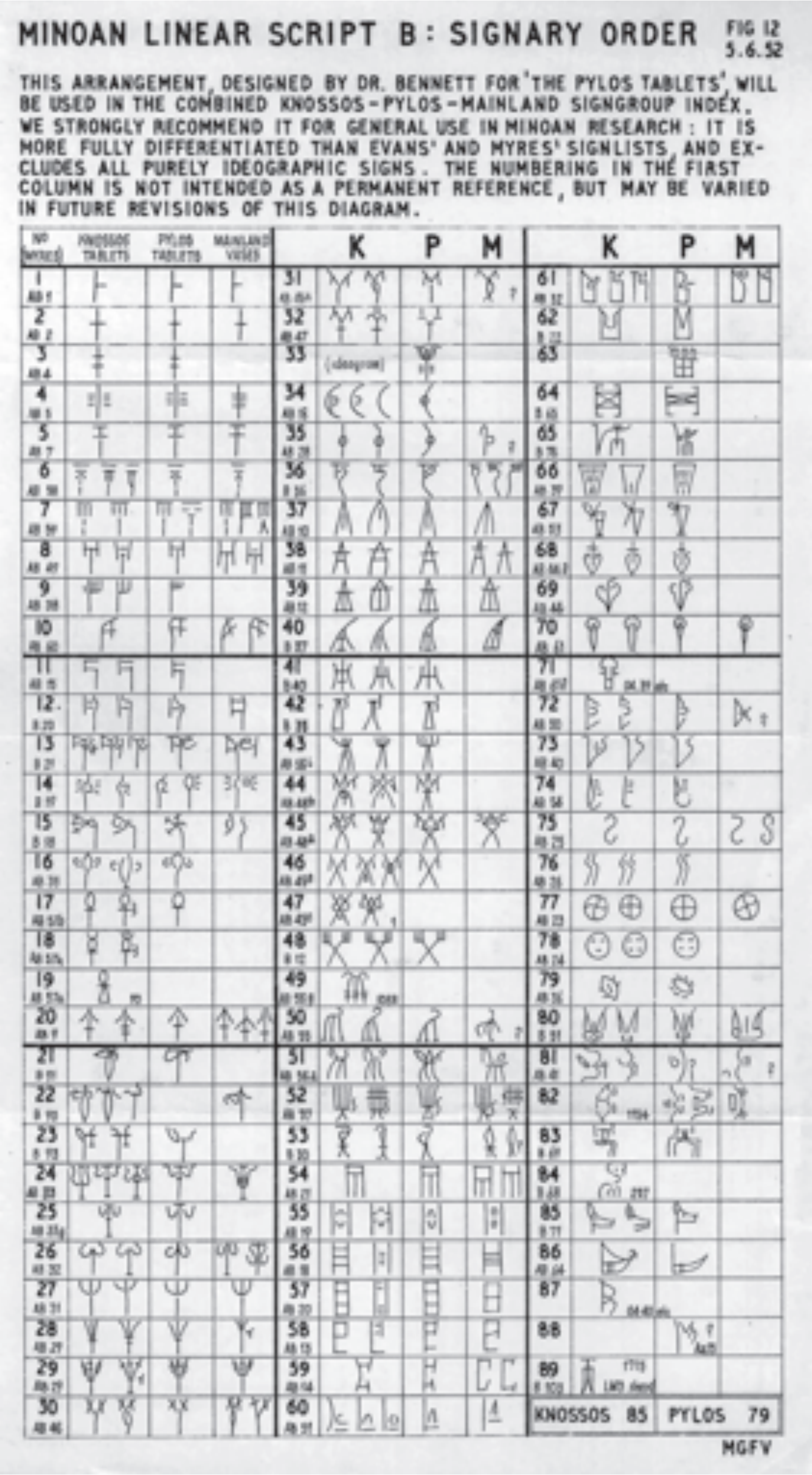
No, I have not received any direct requests for Minoan material. I could not supply them, if I had, even if you agree.

The Pylos material is fascinating, and will probably be useful if I ever get it analyzed. It seems to confirm all my theories--something you won't like at all. At any rate, there's no question any longer about inflection, although the types need analysis. Of course there are various declensions or conjugations, or whatever. Do you want a copy of my copy of the material? It isn't too good, but is all I have, and I made a duplicate. I was pleased to see that it would, with a few rather minor changes, fit quite well into my classification, while Bennett's doesn't suit Knossos at all. But we still haven't gotten together on the classification and order of signs, and I suspect never will. But in that case, my classification is preferable.

My regards to all. I am too tired to write further.

Sincerely
Alice Kober

Figure 5
Michael Ventris's copy of Linear B syllabary in Emmett Bennett's order
(Courtesy of the Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)



MINOAN LINEAR SCRIPT B: SIGNARY ORDER

FIG 12
5.6.52

THIS ARRANGEMENT, DESIGNED BY DR. BENNETT FOR 'THE PYLOS TABLETS', WILL BE USED IN THE COMBINED KNOSSOS-PYLOS-MAINLAND SIGNGROUP INDEX. WE STRONGLY RECOMMEND IT FOR GENERAL USE IN MINOAN RESEARCH: IT IS MORE FULLY DIFFERENTIATED THAN EVANS' AND MYRES' SIGNLISTS, AND EXCLUDES ALL PURELY IDEOGRAPHIC SIGNS. THE NUMBERING IN THE FIRST COLUMN IS NOT INTENDED AS A PERMANENT REFERENCE, BUT MAY BE VARIED IN FUTURE REVISIONS OF THIS DIAGRAM.

KNOSSOS 85 PYLOS 79

MGFV

decipherment of Linear B – and he was to be proved right! Collaboration remains one of the main strengths of Mycenaean studies to this day.
Paper and ink (handwritten), length 33 cm, width 20.5 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

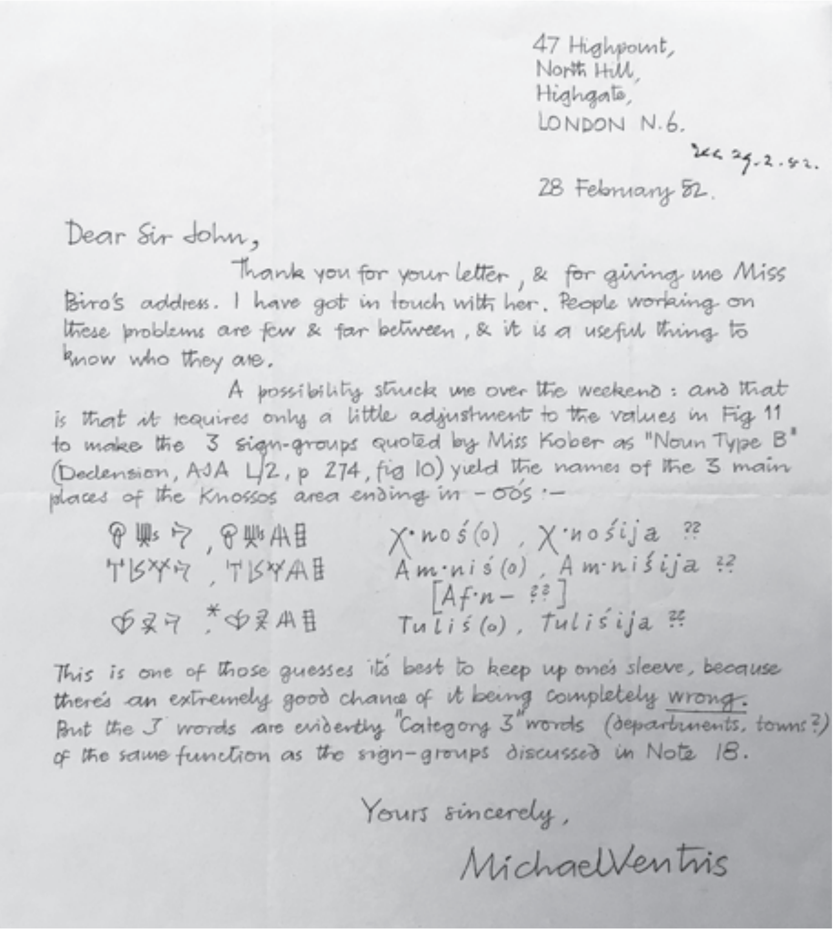
8 *Alice Kober's letter to John Myres, 18 February 1950 (figure 4, p. 117).* Kober wanted to access the Knossos material for her own research on the language of the Linear B. She contacted John Myres and got more than she had bargained for, becoming his chief collaborator in the publication of the *Scripta Minoa*, the Linear B tablets from Knossos, from 1947 to 1950. In the last year of her life, and despite being bedridden most of the time, she continued to work hard, as this letter to Myres suggest. She was also very proud of her work achieving recognition. Her pioneering research on inflection and the development of a grid – to which, unlike Ventris, she was reluctant to assign any phonetic values – paved the way for the decipherment.
Paper and ink (typed), length 30.3 cm, width 18.2 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

9 *Michael Ventris's copy of Linear B syllabary in Emmett Bennett's order, 5 June 1952, figure 5 opposite).* Bennett was an American scholar who was working with documents similar to those displayed in the exhibition. But his material came from the Palace of Nestor at Pylos on mainland Greece. Bennett produced the first accurate list of Linear B signs (signary) that allowed valid statistical analyses to be performed on the script and its language.
Paper and ink (handwritten), length 34.2 cm, width 21.6cm
Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge

10 *The final 'grid' of Michael Ventris (Work Note 17, 20 February 1952, figure 4 in chapter 2, p. 20).* Based on the pioneering work of Alice Kober, this is Ventris's most developed attempt to create a syllabic grid with sound values. The grid proved to be the key to the decipherment. But with Ventris still convinced at this stage, just a couple of months before the dramatic announcement, that the language was Etruscan, he got most of the values shown in the grid of this work note wrong.
Paper, typed and handwritten (copy of an original), length, 32.6 cm, length 19.8 cm
Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge

11 *'A possibility struck me over the weekend' Letter from Ventris to Myres (28 February 1952, figure 6 overleaf).* Michael Ventris, using the work of Alice Kober and making some adjustments of his own, is able to read for the first time 'the names of at least 3 main places of the Knossos area': Knossos, Amnisos and Tulissos. Even at this stage, however, and being so close to the decipherment, he preferred to be cautious: 'This is one of those guesses it's best to keep up one's sleeve, because there's an

Figure 6
Ventris to John Myres,
28 February 1952
(Courtesy of the
Ashmolean Museum,
University of Oxford)



47 Highpoint,
North Hill,
Highgate,
LONDON N.6.

Rec 29.2.52.

28 February 52.

Dear Sir John,

Thank you for your letter, & for giving me Miss Biro's address. I have got in touch with her. People working on these problems are few & far between, & it is a useful thing to know who they are.

A possibility struck me over the weekend: and that is that it requires only a little adjustment to the values in Fig 11 to make the 3 sign-groups quoted by Miss Kober as "Noun Type B" (Declension, AJA L/2, p 274, fig 10) yield the names of the 3 main places of the Knossos area ending in -σός :—

𐀒𐀜𐀰, 𐀒𐀜𐀯𐀍   X·nos(o), X·nośija ??
𐀀𐀖𐀛𐀰, 𐀀𐀖𐀛𐀯𐀍   Am·niś(o), Am·niśija ??
[Af·n– ??]
𐀶𐀪𐀰, *𐀶𐀪𐀯𐀍   Tuliś(o), Tuliśija ??

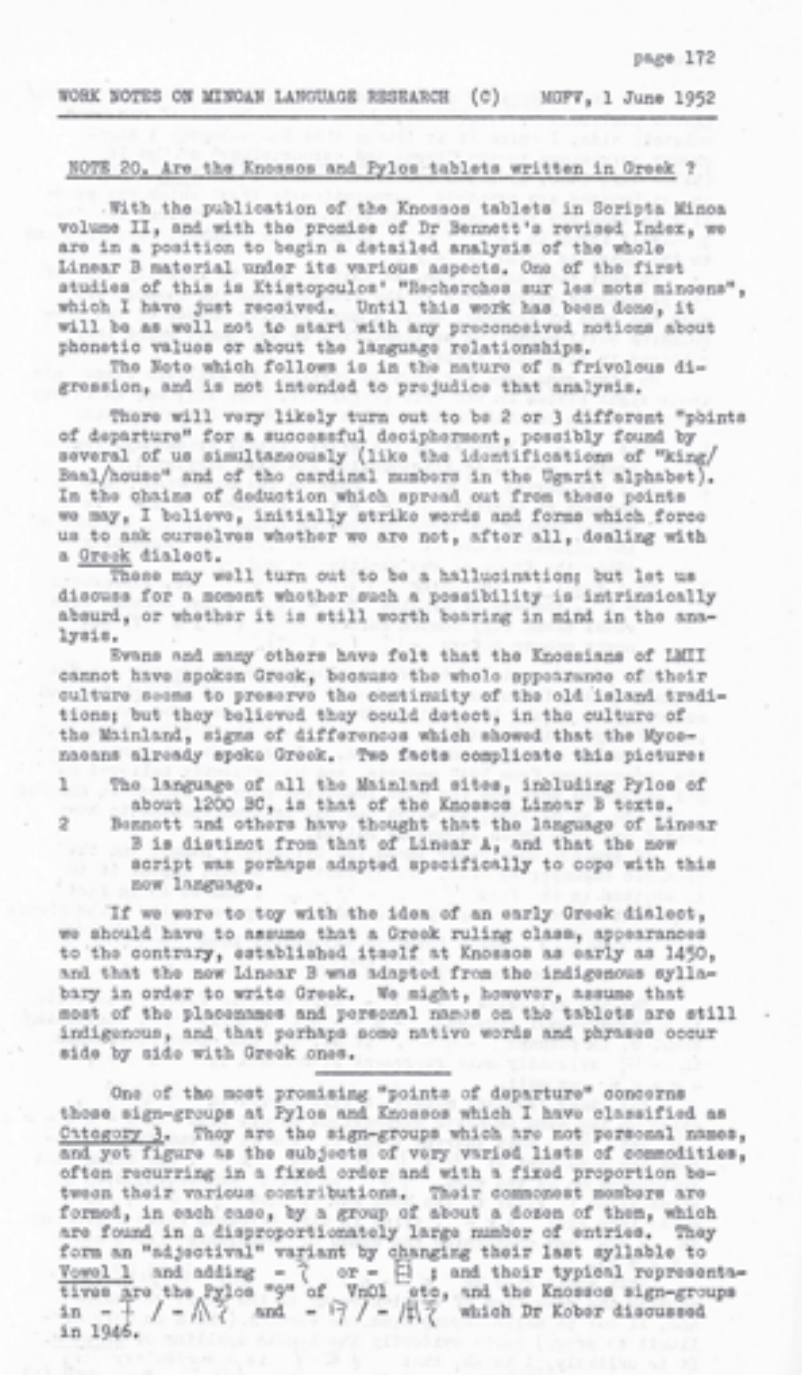
This is one of those guesses it's best to keep up one's sleeve, because there's an extremely good chance of it being completely wrong.
But the 3 words are evidently "Category 3" words (departments, towns?) of the same function as the sign-groups discussed in Note 18.

Yours sincerely,

Michael Ventris

extremely good chance of it being completely wrong'.
Paper and pencil (handwritten), length 22.5 cm, width, 20.5 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

12 *The final Work Note of Michael Ventris prior to the announcement of the decipherment of Linear B (Work Note 20, 1 June 1952, figure 7).* Ventris recorded and circulated twenty 'Work Notes'to scholars working on Linear B. Entitled 'Are the Knossos and Pylos tablets written in Greek?', Work Note 20 is the most dramatic. Although he called this possibility a 'frivolous digression', and that the identification of a few Greek words 'may well turn out to be a hallucination', a month later he astounded the world with his announcement on the BBC's Third Programme (1 July 1952) that the language of Linear B must after all be 'Greek – a difficult and archaic Greek, seeing that it's 500 years older than Homer and written in a rather abbreviated form, but Greek nevertheless'.
Paper, typed and handwritten (copy of an original), length 33 cm, width 20.4 cm
Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge.



page 172

WORK NOTES ON MINOAN LANGUAGE RESEARCH (C) MGFV, 1 June 1952

NOTE 20. Are the Knossos and Pylos tablets written in Greek ?

With the publication of the Knossos tablets in Scripta Minoa volume II, and with the promise of Dr Bennett's revised Index, we are in a position to begin a detailed analysis of the whole Linear B material under its various aspects. One of the first studies of this is Ktistopoulos' "Recherches sur les mots minoens", which I have just received. Until this work has been done, it will be as well not to start with any preconceived notions about phonetic values or about the language relationships.

The Note which follows is in the nature of a frivolous digression, and is not intended to prejudice that analysis.

There will very likely turn out to be 2 or 3 different "points of departure" for a successful decipherment, possibly found by several of us simultaneously (like the identifications of "king/Baal/house" and of the cardinal numbers in the Ugarit alphabet). In the chains of deduction which spread out from these points we may, I believe, initially strike words and forms which force us to ask ourselves whether we are not, after all, dealing with a Greek dialect.

These may well turn out to be a hallucination; but let us discuss for a moment whether such a possibility is intrinsically absurd, or whether it is still worth bearing in mind in the analysis.

Evans and many others have felt that the Knossians of LMII cannot have spoken Greek, because the whole appearance of their culture seems to preserve the continuity of the old island traditions; but they believed they could detect, in the culture of the Mainland, signs of differences which showed that the Mycenaeans already spoke Greek. Two facts complicate this picture:

1 The language of all the Mainland sites, inbluding Pylos of about 1200 BC, is that of the Knossos Linear B texts.
2 Bennott and others have thought that the language of Linear B is distinct from that of Linear A, and that the new script was perhaps adapted specifically to cope with this new language.

If we were to toy with the idea of an early Greek dialect, we should have to assume that a Greek ruling class, appearances to the contrary, established itself at Knossos as early as 1450, and that the new Linear B was adapted from the indigenous syllabary in order to write Greek. We might, however, assume that most of the placenames and personal names on the tablets are still indigenous, and that perhaps some native words and phrases occur side by side with Greek ones.

One of the most promising "points of departure" concerns those sign-groups at Pylos and Knossos which I have classified as Category 3. They are the sign-groups which are not personal names, and yet figure as the subjects of very varied lists of commodities, often recurring in a fixed order and with a fixed proportion between their various contributions. Their commonest members are formed, in each case, by a group of about a dozen of them, which are found in a disproportionately large number of entries. They form an "adjectival" variant by changing their last syllable to Vowel 1 and adding -𐀊 or -𐀍 ; and their typical representatives are the Pylos "9" of Vn01 etc, and the Knossos sign-groups in -𐀰 / -𐀯𐀊 and -𐀵 / -𐀴𐀊 which Dr Kober discussed in 1946.

Figure 7
The last Work Note of Michael Ventris
(Courtesy of the Mycenaean Epigraphy Group, Faculty of Classics, University of Cambridge)

13 *Letter from Michael Ventris to John Myres that Linear B is written in Greek (received 18/06/1952, figure 6 in chapter 1, p. 11).* Ventris, who for a long time was convinced that the language of Linear B was Etruscan, announced to Myres his breakthrough discovery. His surprise is evident in this letter.
Paper and ink (handwritten), length 33 cm, width 20.5 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

14 *The 'independent proof'. Letter from Michael Ventris to John Myres about Pylos tablet no. 641 (19 May 1953, figure 7 in chapter 2, p. 26).* Following the announcement of the decipherment on the radio on 1 July 1952, Ventris needed more evidence to prove the validity of the sound values he had assigned to some of the Linear B signs. Fortuitously this 'independent proof' came soon after. Carl Blegen, the excavator of Pylos, studying a tablet that had recently been unearthed during his excavations (PY Ta 641) applied the phonetic sounds to the signs he could read. So astonished was Blegen by the excellent correspondence between the ideograms representing different types of vessels and the undeniably Greek words describing them (e.g. tripod, describing a three-legged vessel) that he wrote to Ventris: 'all this seems too good to be true. Is coincidence excluded?' It was indeed. The reading of this tablet proved to all, but the most sceptical, that Ventris's decipherment was correct.
Paper and ink (typed and handwritten), length 33 cm, width, 20.5 cm
John Linton Myres Archive, Ashmolean Museum, University of Oxford

15 *A complete clay tablet inscribed in the Linear B script from the palace at Knossos (figure 4 in chapter 6, p. 30).* It records the transfer of coriander, an ingredient used in the perfume industry. The palace controlled major industries like textile production and the manufacture of perfumed olive oil. The transfer here is between a man named Kyprios (Cypriot) and another person, named Twinon, probably the perfumer. The quantity of coriander recorded in this tablet would be enough to treat 5,000 litres of oil, a massive production suggesting that perfumery was not just for internal consumption but also for export. Knowledge of the quality and scale of production are two great insights gained through the decipherment of Linear B, despite the fragmentary and haphazardly preserved nature of our evidence.
Baked clay, around 1375 BC, length 12.1 cm, width 1.4 cm
GR.1.1911, Fitzwilliam Museum, University of Cambridge

16 *Partially preserved clay tablet from the palace at Knossos recording ritual and drinking vessels in the shape of a bull's head and of handled cups (plate 4).* These vessels, part of the palace inventories, might have been used in banquets or religious festivals. They had a small hole at the snout for pouring liquid offerings, such as wine, perfumed oil or honey. The cups are described as being made of gold. Simpler versions, made of clay, are commonly attested in tombs and settlements.

Baked clay, around 375 BC, length: 6 cm, width 4.6 cm
AN1896-1908/AE.2031, Ashmolean Museum, University of Oxford

17 *Partially preserved Linear B tablet from the palace at Knossos recording short swords ('pa-ka-na') (plate 5).* This document reads 'so many swords' followed by the sign for 'sword' and then the number '50'. More swords appear in other documents. The palace was well equipped for battle.
Baked clay, around 1375 BC, length 9.9 cm, width 2.6 cm.
AN1938.706, Ashmolean Museum, University of Oxford

18 *Fragment of a Linear B tablet from the palace at Knossos recording two body armours and a wheeled chariot (the latter only partly visible, plate 6).* The palace had control over the production of chariots and armour. Body-length armours are known as *to-ra-ke* in Linear B. A few examples are attested archaeologically giving us precious insights into the making of these defensive weapons.
Baked clay, around 1400 BC, length 3.5 cm, width 2.5 cm
AN1938.860, Ashmolean Museum, University of Oxford

19 *Fragment of a Linear B tablet from the palace at Knossos recording one wheeled chariot and a horse (the latter only partly visible, plate 7).* In Linear B the chariot was called *i-qi-ja*, 'vehicle drawn by horse(s)'. The surviving tablets from Knossos describe the manufacture of chariots at various places across the island of Crete. Making a chariot is a complex process, with its construction requiring accuracy and expertise. Although no chariot survives archaeologically, they are well attested on wall paintings and decorated pots. From the Linear B documents, we learn about the different materials used, their decoration, and technology. They are also recorded at different stages of assembly (e.g. with or without wheels). Horses were used to draw chariots. In the tablets and also on wall paintings and decorated pots they appear having elaborate braided manes. Part of this elaborate braided mane is visible at the right end of this tablet. Some horses received a proper burial, suggesting their special status either in relation to the funeral or as part of their ceremonial position in society.
Baked clay, around 1400 BC, length 4.2 cm, width 2 cm
AN1938.859, Ashmolean Museum, University of Oxford

20 Signet ring engraved with two figures driving a chariot drawn by Cretan wild goats (plate 8). Said to come from Spiliaridia near Avdou, central Crete. Representations of chariots are also attested on Linear B documents as well as on wall paintings and decorated pots. Chariots appear to have been used in ceremonial display and in connection with hunting.
Agate, around 1450–1375 BC, 2.8 cm x 2.1 cm (bezel)
AN1938.1051. Ashmolean Museum, University of Oxford

21 *Fragment of a Linear B tablet recording a water-jug from Knossos (plate 9).* The scribe has recorded here a jug on top of which he has placed the sign for */u/* an abbreviation standing for */húdōr/* ('water' in Greek). These water jugs were known as *hudria* in classical times. The numerical system in Linear B is decimal. A vertical line stands for '1'; a horizontal line stands for '10'; and a circle stands for '100'.
Baked clay, about 1375 BC, length 3.5 cm, width 1.5 cm
AN1938.855. Ashmolean Museum, University of Oxford

22 *Complete Linear B tablet from the palace at Knossos recording sheep at a place called 'da-ti-jo' (plate 10).* The first line records 28 male and 22 female sheep, while in the second line a debt is recorded of 50 sheep. Numbers always round to '100', suggesting that specific amounts were required at each inspection. The textile industry was one of the most important for the palace at Knossos. Although the various stages of the textile production are recorded, from herding and shearing to dyeing the wool and producing different types of textiles, the tablets are silent when it comes to the distribution of the finished products. Over 80,000 sheep in more than 30 locations, recorded by a single scribe on 600 tablets, suggest that production was not just for internal consumption but also for export. At least 900 female weavers, supported with rations of grain and figs from palace-controlled stores, at workshops in about 15 different locations across much of Crete were involved in the production of textiles. Around 1375 BC.
Baked clay, about 1375 BC, length 11.6 cm, width 2.3 cm
AN1938.708, Ashmolean Museum, University of Oxford

23 *Page-shaped Linear B tablet, partially preserved, from the palace at Knossos (plate 11).* Once described by Arthur Evans as listing 'concubines', this tablet records, by name, women workers most likely involved in the textile industry of the palace. Occasionally these women are accompanied by 'boys' and 'girls', perhaps their children. In line seven a subtotal is given, *to-sa* (*tossai*, 'so many' in ancient Greek), followed by the symbol for 'woman' and the number 45. This total is followed by 5 girls (*ko-wa*) and 4 boys (*ko-wo*).
Baked clay, around 1375 BC, length 10.5 cm, width 10.7 cm
AN.1910.218, Ashmolean Museum, University of Oxford

24 *Partially preserved Linear B tablet from the Palace at Knossos recording the allocation of rations to women (plate 12).* The first line records rations to women of Knossos (*ko-no-si-ja*), the second to women of Amnisos, a port of Knossos (*a-mi-ni-si-ja*) and the third to women of Phaistos (*pa-i-ti-ja*)in southern Crete. These are monthly rations as indicated by the half-moon sign. The amounts distributed here would be enough to feed 500 women for a month (with a very modest amount of grain for each day). The tablet is also inscribed at the back where we learn that these women are *asketriai* (decorators), associated with the palace's textile industry. These adjectives, derivatives of place names, played a role in the

decipherment of Linear B (see chapter 2).
Baked clay, around 1375 BC, length:8 cm, width 0.6 cm
AN1910.214, Ashmolean Museum, University of Oxford

25 F*ragment of a Linear B tablet with joins at the Herakleion Museum in Crete (plate 13).* Discovered at the palace at Knossos, it records grain quantities. Grain is the staple food allocated to workers. Based on the handwriting, very clear in this instance, we call the anonymous people who wrote the documents 'scribes'.
Baked clay, around 1375 BC, length 6.8 cm, width 4.5 cm
AN1938.710, Ashmolean Museum, University of Oxford

26 *Partially preserved Linear B tablet from the palace at Knossos (plate 14).* It probably records rations of barley (*ki-ri-ta*) to groups of women, one coming from Chania in west Crete (recorded as *ku-do-ni-ja* in the top line).
Baked clay, around 1375 BC, length 17 cm, width 3.6 cm
AN1910.215.Ashmolean Museum, University of Oxford

27 *Unique prototype writing desk (see plate 15).* Designed by Hungarian-born architect and designer Marcel Breuer in 1936, the desk was commissioned by Michael Ventris's mother Dorothea, a committed collector of contemporary art and design, for her home, Flat 47 in Highpoint I, a block of flats in Hampstead, London. Highpoint was itself a modernist building designed by the Russian-born architect Bertold Lubetkin. The desk remained in the flat until the 1950s when Michael Ventris designed a new home for himself, incorporating the suite of furniture commissioned by his mother. It is thought that it was at this desk that Michael Ventris was working when he first deciphered Linear B.
Sycamore veneered laminated board, chromium-plated tubular metal, glass top, rubber fittings and linoleum, 1937, *height 74 cm, width 122 cm, depth 61 cm*
W.64:1 to 9-2002.Victoria and Albert Museum

28 *Replica of a Linear A tablet (not illustrated).* Although Linear A is an undeciphered script, it is generally believed that the language (or languages) it was used to record is or are unrelated to Greek. At the moment, we still have relatively few documents for any credible decipherment to take place. Nevertheless, we can 'read' some of these tablets as most of the signs, and most likely also sound values, of Linear A are the same as with Linear B. This tablet appears to record olive oil, wool and figs at a place called *qa-ti-da-te* which appears as a heading in the first, top, line. The original tablet, discovered at Hagia Triada, is now in the Herakleion Museum in Crete.
Plaster cast, twentieth century, length 7.2 cm, width 4.3 cm
M60, Museum of Classical Archaeology, Faculty of Classics, University of Cambridge

The Second World War: Computers and the Future

1 *Enigma machine with plug board, in box (plate 16).* The Enigma is an electromechanical cipher machine, which has been described as one of the most famous cipher machines of all time. On 2 February 1942 the German U-boats increased security overnight by switching to new four rotor Enigma machines. This change locked the British codebreakers out of the U-boat information for nine months. These machines were exclusive to the U-boats and breaking the code provided the allies with important information that allowed supplies from the USA to cross the Atlantic. The wiring inside the fourth rotor was deduced by Alan Turing, and the task of breaking of U-boat information was shared between the USA and Britain. This machine was manufactured in 1944 and bears the serial number M18273.
Height 46.1 cm, width 28.6 cm, depth 51.7 cm, weight 11.5 kg
Crown Copyright 2017

2 *BID 08/2 Typex Mark 22 cipher machine, in wooden carrying case and lid (plate 17).* Another British cipher machines during the Second World War was the Typex. These machines were based on the general logic of the Enigma machines, although they more secure as the Typex contained five rotors instead of three. The rightmost two rotors were statics and served a similar function to the Enigma plugboard. The leftmost three rotors would turn, but did so more frequently than Enigma making the pattern of cipher less predictable. The Typex could also be connected to teleprinters and contained two printers, one for the cipher text and one for the plain text, rather than using a lampboard. The first Typex machines were distributed in 1937. The year of manufacture for this Typex Mark 22 machine is unknown.
Late Second World War, height 42.0 cm, width 89.5 cm, depth 60.0 cm, weight with lid 84 kg, weight without lid 68 kg
Crown Copyright 2017

3 *Alan Turing (plate 18).* A photograph of the mathematician sitting on the porch of his family house.
Photograph
AMT/K/7/36, King's College Library, Cambridge

4 *A report from Sherborne, Alan Turing's school (plate 19).* Where he is stated as a first-class mathematician. Alan Turing's school reports give a fascinating insight into the young mathematician. Several of his teachers describe his work as 'messy'. It became apparent that Turing's interests were exclusively in science and mathematics, much to the concern of his English and French teachers. As he progresses we see some improvement in the subjects that Turing tolerated, but his mathematics and science teachers begin to recognize Turing as a potential genius.
Paper, 21.1 cm x 29.8 cm
AMT/A/46/16, King's College Library, Cambridge. Permission to reproduce courtesy of Sherborne School, where original documents are also stored.

5 *'Mathematical recreations', by William W. Rouse Ball (Macmillan, London, 1928, plate 20).* This book was given to Alan Turing as a prize. Not many of Turing's friends at school shared his scientific interests. One boy who did was Christopher Morcom. Unfortunately, Morcom died at a young age. It is fitting then that Turing was the first winner of Sherborne School's Christopher Morcom Science Prize for his investigation into the Iodine Clock Reaction that the boys had discussed together. The prize was a book on recreational mathematics, a popular book that inspired many young mathematicians. The last chapter of this book is about codes and ciphers, which inspired Turing to send messages to his friends using some of the ideas in the book (pages 310–311 are illustrated here). The book also gives a warning about the use of mechanical cipher machines and how they are unlikely to replace pen and paper methods.
Book, 19.8 cm x 13.4 cm x 2.7 cm
AMT/B/35, King's College Library, Cambridge

6 *A paper by Alan Turing 'On Computable Numbers', (not illustrated).* The Decision Problem (otherwise known as the *Entscheidungsproblem*), asks whether there is a method that can decide if a mathematical statement is provable. Turing's paper shows there is no such method by describing a problem that cannot be resolved. Turing's proof introduces the idea of a universal computing machine which contains many of the fundamental concepts of the modern computer.
Proceedings of the London Mathematical Society, December 1936

7 *A letter of Alan Turing addressed to his mother Sara Turing written in October 1936 (plate 22).* Alan Turing wrote this letter just when he was embarking on his PhD in Princeton. In the letter Turing muses on the most general type of code possible, while he also considers the possibility of selling his ideas to HM Government, but is 'rather doubtful about the morality of such things'.
Paper, handwritten in ink, height 23.3 cm x width 15.0 cm
AMT/K/1/43, King's College Library, Cambridge

8 *Blueprint of the Zeta Function Machine, designed by Alan Turing in 1939 (plate 21).* This machine calculates the zeros of the Riemann zeta function, one of the most important problems in mathematics. This is an early example of Turing's use of machines to solve complex problems but construction of it was abandoned due to the outbreak of war. In 1950 Turing used one of the world's first computers, the Manchester Mark I to perform this calculation instead.
Paper
AMT/C/2, King's College Archives, Cambridge, University of Cambridge.

9 *A letter of Alan Turing to his mother, from Bletchley (plate 23).* This is a rare letter from Turing written during his stay at Bletchley. In this, Turing describes returning to Bletchley to great excitement over a near miss by a

bomb. The letter also mentions Bob, an Austrian refugee that Turing had sponsored in order to complete his studies in England. Turing's friend Fred Clayton was a classicist who between 1935 and 1937 had studied in Vienna and Dresden and had experienced the rise of Nazism. Clayton together with Turing decided to sponsor two young refugee boys, Karl and Bob and made arrangements for them to attend Rossall school in Lancashire.
Paper, handwritten in ink, height 22.7 cm x width 17.7 cm
AMT/K/1/71, King's College Library, Cambridge

10 *Alan Turing with his classicist friend Fred Clayton and two young Austrian boys, sailing at Bosham, Sussex in August 1939 (plate 24).* Behind Turing is Fred Clayton, another young Fellow of King's College, Cambridge, and between them are two Jewish refugee boys, Robert and Karl from Austria and Germany respectively. Alan Turing and Fred Clayton had helped them to find asylum in Britain at the time Nazism was rising in Germany.
Photograph
1945063a, REX/Shutterstock, image library

11 *Alan Turing running, December 26, 1946 (plate 25).* Turing ran at an event while he was working for the National Physics Laboratory (NPL), London. He joined the NPL in 1945, where he worked on the Automatic Computing Engine (ACE) till 1947. Turing was also an avid runner and his marathon time was considered world class.
Photograph
AMT/K/7/8, King's College Library, Cambridge

12 *Transcribed note of Alan Turing on 'how to solve a solitaire' (plate 26).* This is a transcription of a handwritten note from Alan Turing to Maria, the young daughter of his analyst. After his conviction for gross indecency in 1952, Turing began to see psychologist Franz Greenbaum. Turing and Greenbaum became friends, and his daughter remembered Turing fondly as a warm and friendly visitor, who would sit on the carpet and talk to her while she played games. This letter to Maria, written in the Summer of 1953, describes how to win the game of solitaire.
Paper, handwritten in ink, height 25.3 cm x width 20.3 cm
AMT/K/1/83, King's College Library, Cambridge

13 *Teaspoon with handwritten label by Sara Turing (plate 27).* Turing was found dead on 7 June 1954 at the age of forty-one. An inquest determined he died of cyanide poisoning, and it is widely believed that Turing committed suicide. Others have disputed this conclusion and believe Turing's death was accidental as Turing often performed chemical experiments at home. This teaspoon was labelled by Alan's mother, 'This is the spoon which I found in Alan Turing's laboratory. It is similar to the one which he gold-plated himself. It seems quite probable he was intending to gold-plate this one using cyanide of potassium of his own manufacture.'

Silver, card and cord, 12.7 cm x 2.5 cm x 0.9 cm, paper label, 11.9 cm x 6.1 cm
AMT/A/12, King's College Library, Cambridge

14 *Correspondence regarding the inauguration of the Alan Turing Award (plate 28).* The award was instituted by the Association for Computing Machinery in 1966, and has been awarded yearly ever since to computing experts for contributions 'of lasting and major technical importance to the computer field', including Sir Tony Hoare in 1980, a contributor to this exhibition and volume. The Turing Award is generally recognized as the highest distinction in computer science and as the 'Nobel Prize of computing'.
Paper, typed, 28.0 cm x 21.7 cm
AMT/A/24, King's College Library, Cambridge.

15 *Photograph of Bill Tutte as a student at Trinity College Cambridge (figure 3 in chapter 9, p. 89).*William (Bill) Tutte was a recent graduate when he was recruited to work at Bletchley Park, but his contributions during the war are as important as those by Alan Turing. He became a member of the Trinity College Mathematics Society where he gained a reputation as a puzzle solver and was recommended to Bletchley Park. Tutte was part of the Research Station, the part of Bletchley Park dealing with as yet unsolved problems. Tutte made the first breakthrough on the Lorenz cipher machine, deducing its nature without ever seeing the machine itself. Later he developed a method to break Lorenz which was put into practice via the code breaking machine Colossus, built by Tommy Flowers.
Photograph
FA II.34 [2], Trinity College, University of Cambridge

16 *Quantum Key Distribution system (plate 29).* This illustrates the future of cryptography. Every cipher requires a key, a kind of secret password that allows us to code and decode messages. If the sender uses a different, and randomly generated, key for each letter of the message then this randomness makes the code mathematically impossible to break. Traditionally, the problem with this kind of system was transmitting the key to the receiver without the key being intercepted. Quantum Key Distribution solves this problem by transmitting the key via particles of light through fibre optic cables. Due to the nature of these particles of light, any attempt to spy on this system will be detected.
Various materials, width 48.5 cm x height 60.0 cm x depth 9.0 cm
Andrew Shields, Toshiba Research, Cambridge

Notes

Chapter 1

[1] Evans 1943, 309–10. On Evans's progressive interest in Aegean archaeology see Galanakis 2014.

[2] Bennet 2014, 127.

[3] On Myres's trip and his interest in excavating Knossos see Brown 1986.

[4] Evans 1894, 813.

[5] Perhaps the σήματα λυγρά (Iliad 6.168, the only reference to writing in Homer) or the mysterious documents found at Knossos in Nero's time, as Evans first proposed, could refer to the Linear system of writing which disappeared following the collapse of palatial administration in the Aegean around 1200 BC.

[6] Sayce 1896, 149.

[7] Evans 1899–1900, 56.

[8] Cowley 1927.

[9] Evans was also nearly convinced that Linear B could write Greek: when he applied the Cypriot sound values 'po' and 'lo' on two of its signs that looked very similar. The word that was created, *polo* = φόλος, 'foal(s)' in Greek, preceded in Linear B documents from Knossos a horse's head which would seem to strengthen further Evans's 'borrowing'. Yet he rejected the connection, mostly based on his firm conviction that the Minoans could not have spoken and written in an archaic form of Greek but in an unrelated, 'Cretan' language. See Robinson 2002, 34–7.

[10] Evans 1935.

[11] Pope 1975, 154 and also pp. 146–8.

[12] Tylor 1873, 233: 'When we study pictures and gestures . . . we can mostly see at a glance the direct relation between the outward sign and the inward thought which it makes manifest'; see also Tylor 1881, esp. chapters 4, 6 and 7.

[13] Evans 1928, 321. On the controversy see Galanakis 2015.

[14] University of Cincinnati archives, Carl W. Blegen Papers, Folder 119, Wace to Blegen, 12 August, 1940.

[15] The display included a replica of the Phaistos disk, a series of clay tablets from Evans's collection (now at the Ashmolean Museum in Oxford), tables with lists of signs of the advanced Minoan linear script and a series of mainland signs, also of the 'Linear class'. According to Evans the presence of the latter appeared to suggest that 'in the 14th century BC, the language of the intrusive population from Minoan Crete was still spoken in the chief civic centres on the Mainland' (Evans 1936, 27).

[16] Robinson 2002, 21–3.

[17] Arthur J. Evans Archive, Ashmolean Museum, University of Oxford, Ventris to Evans, Easter (March) 1940.

[18] John L. Myres Archive, Ashmolean Museum, University of Oxford, Ventris to Myres, received 18 June 1952.

[19] John L. Myres Archive, Ashmolean Museum, University of Oxford, Chadwick to Myres, 9 July 1952. Chadwick further noted that '[Mr Ventris] seems to be finding it hard to convince Greek scholars that the language really is Greek . . . Mr Ventris seems very glad to have found a philologist to help him, and I am glad to say that I have already been able to offer some suggestions' (John L. Myres Archive, Ashmolean Museum, University of Oxford, Chadwick to Myres, 18 July 1952).

[20] Ventris 1952, 58.

[21] Ibid.

Chapter 2

1 Davies 1987.
2 Evans 1935.
3 Evans 1952.
4 Chadwick 1992, 26–32.
5 Briggs 2011.
6 Fox 2013.
7 E.g. Kober 1946 and 1948.
8 Kober 1948, 103.
9 Robinson 2002.
10 Ventris and Sacconi 1988.
11 Quoted in Fox 2013, 103.
12 Ventris and Sacconi 1988.
13 Ventris 1952.
14 Killen and Morpurgo Davies 2002.
15 Ventris and Chadwick 1953.
16 Ventris and Chadwick 1956.
17 Chadwick 1992.

Chapter 3

1 For those interested in finding more, beyond this exhibition catalogue, the excellent three-volume companion of Duhoux and Morpurgo Davies (2008–14) offers the most detailed treatment of Mycenaean Greek texts and their world ; see also Del Freo and Perna (2016).
2 Haskell et al. 2011.
3 The equivalent transport container in the eastern Mediterranean was a vessel called the Canaanite jar, similar in concept to later Graeco-Roman amphoras; their capacities ranged from seven to twenty-seven litres (Aruz et al. 2008, 317–20).
4 Judson 2013.
5 E.g. Jones 2015.
6 Killen 1964.
7 Nosch 2014.
8 Halstead 1993.
9 It is worth noting that the texts only distinguish two forms of grain, almost certainly wheat and barley, while the archaeobotanical record not only documents different types of wheat, but also a broad range of pulse crops (Halstead 1995).
10 Cf. Bennet 2008, 157–9.
11 A fragmentary marble table top with indentations for inlays was found in Carl Blegen's excavations at the palace at Pylos in 1954 (Blegen 1955, 34).
12 On Mycenaean feasting in general, see Wright 2004.
13 There are several others, but uncertainties remain about their identification with specific later sites (McArthur 1993).
14 Cf. Nakassis 2013.
15 Finley 1957, 159.
16 Postgate 2013.
17 E.g. Feldman 2006 and Van de Mieroop 2000.

Chapter 4

1 See, for example, the chapter by Roeland P.-J. Decorte in Steele 2017.
2 Steele and Meißner in Steele 2017.
3 See for example the chapter by Miguel Valério in Steele 2017.
4 Ferrara 2012–13.
5 Steele 2013, chapter 2.
6 Steele 2017.

Chapter 5

1 http://wiki.digitalclassicist.org/Main_Page.
2 http://people.ku.edu/~jyounger/AegeaNet/.
3 http://minoan.deaditerranean.com/linear-b-transliterations/.
4 https://www2.hf.uio.no/damos/ *Dāmos*, a word mentioned in Mycenaean Greek, translates as 'district', 'community' or 'people'.
5 http://liber.isma.cnr.it/.
6 http://sirarthurevans.ashmus.ox.ac.uk/collection/linearb/images.php.
7 Freely available from its developer, the nonprofit organization Cultural Heritage Imaging (CHI): http://culturalheritageimaging.org/What_We_Offer/Downloads/View/.
8 http://calibra.classics.cam.ac.uk/.
9 https://arachne.dainst.org/.
10 Freely available at the Internet Archive: https://archive.org/details/scriptaminoawrit02evanuoft and http://digi.ub.uni-heidelberg.de/diglit/evans1952.
11 http://www.cervantesvirtual.com/bib/portal/diccionariomicenico/.
12 http://www.palaeolexicon.com/Languages/Index.
13 http://www.people.ku.edu/~jyounger/.
14 All are available at the 'Collections de l'Ecole française d'Athènes en ligne': http://cefael.efa.gr/site.php.
15 Freely available at the Internet Archive: https://archive.org/details/scriptaminoawrit01evanuoft and http://digi.ub.uni-heidelberg.de/diglit/evans1909.

16 The linguistic annotation is not yet available online, but will be published and made available for searches in a forthcoming version of the database.

17 Snyder et al. 2010: 1048.

18 DOI:10.1093/acref/9780199545568.001.0001.

19 http://referenceworks.brillonline.com/cluster/New%20Pauly%20Online.

20 http://referenceworks.brillonline.com/browse/encyclopedia-of-ancient-greek-language-and-linguistics.

21 http://lila.sns.it/mnamon/.

22 For an overview of the archive's material: http://sirarthurevans.ashmus.ox.ac.uk/introduction/ The material that has so far been digitized resides in Digital Bodleian, a portal of the Bodleian Library of the University of Oxford: http://digital.bodleian.ox.ac.uk/.

23 https://repositories.lib.utexas.edu/handle/2152/20176. A PDF file with a catalogue of the archive of Ventris' own papers, housed by the Institute of Classical Studies, can be found at: http://sas-space.sas.ac.uk/id/eprint/330.

24 https://repositories.lib.utexas.edu/handle/2152/15875.

25 https://repositories.lib.utexas.edu/handle/2152/32270.

26 *Mnamon* also provides a review of online resources for the Aegean scripts and it can be used as a companion website to the present text.

27 http://www.classics.cam.ac.uk/seminars/projects/mycep/links.

28 https://www.aegeussociety.org/en/.

29 http://classics.uc.edu/nestor/ Some volumes of the Mycenaean bibliography 'Studies in Mycenaean Inscriptions and Dialects' (SMID) are available as PDFs from PASP: https://repositories.lib.utexas.edu/handle/2152/16096.

30 http://www.aegean-museum.it/.

Chapter 6

1 Smith 2011, 5–7.

2 Quoted in Richmond 2001, 87.

3 See Hodges 1992, 166–7; Singh 2000, 127–35.

4 See Singh 2000, 149–58.

5 CIL is often explained as the initials of the unknown operator's girlfriend. However, to classicists, CIL invariably refers to the Latin epigraphy corpus, *Corpus Inscriptionum Latinarum.* It is an entertaining thought (if not particularly likely one) that the operator was a Latin epigraphist.

6 Hunter 2003.

7 Ibid.

8 Wilkinson 2001, 61.

9 Chadwick, *Memoirs,* 60.

10 According to Josh Cooper, quoted in Batey 2009, 49.

11 Quoted in Lee and Holtzman 1995, 39.

12 Quoted in Smith 2011, 76–7.

13 McKay 2013, 95.

14 Chadwick, *Memoirs*, 43.

15 Ibid., 74.

16 Erskine and Smith 2011.

17 Wilkinson 2001, 63.

18 Batey 2009, 20.

19 Chadwick 1958, 40.

20 See Burman 2012.

21 Hodges 1992, 161; Stripp 2012, 15; Andrew 1985, 34.

Chapter 7

1 Ancient cryptographic systems indeed assumed that the algorithm is unknown to enemies; however, even as early as 1883 it has been assumed that the algorithm is known; see chapter 10.

2 Until recently, the sender and the receiver had to share the same key for encryption and decryption. Today, we have public-key cryptographic systems, which use different keys for encryption and decryption; see chapter 10. In addition to message encryption, public-key cryptography also enables message signing.

3 More precisely, testing should require on average half of the possible encryption keys.

4 Clark 1988

5 The block cipher typically works on short messages or fragments of the original message; many applications of the block cipher are required to encrypt a long message.

6 One-way functions are too slow to encrypt long messages; typically they are used in conjunction with block ciphers.

7 Szekeres et al. 2013 and Aleph One 1996. A look at the attacks presented at Black Hat Briefings (https://www.blackhat.com), DEF CON (https://www.defcon.org/), and elsewhere attests to the creativity of those system hackers.

8 Guri et al. 2015.

9 See Hastings 2016, 70.

10 See https://www.britannica.com/technology/

ENIAC.

11 See https://www.britannica.com/topic/Turing-machine.

12 See https://www.britannica.com/technology/Turing-test.

13 Ellis 1969.

14 Rivest, Shamir, and Adleman 1978.

15 Diffie and Hellman 1976.

Chapter 10

We are grateful to Professor Ross Anderson for many insightful comments and corrections. Any remaining inaccuracies are of our own making and breaking.

1 The Colossus Mark 2 was clocked at 25kHz. We estimate the unclocked Mark 1 at 5kHz as it was 5 times slower: https://en.wikipedia.org/wiki/Colossus_computer#Design_and_construction.

Thus, the number of instruction of Mark 1 in two years (with one a leap year is): $5{,}000 * 60^2 * 24 * (366+365) = 315{,}792 * 10^{6.}$

For the iPhone 7 with its two active core the number of instructions in two minutes is: $2 * 2{,}340 * 10^6 * 60 * 2 = 561{,}600 * 10^{6.}$

2 25Mbps *60/8 = 187.5 *10^6.

3 This means that the number of guesses was halved 72 times, as $2^{128}/2^{72}=2^{56}$.

4 The authors would also like to thank Dr Panayotis Vryonis for giving us permission to use the idea of keys that turn in different directions (see further reading).

5 A sign could be an alphabetical character, but it also could represent frequently used words or numbers.

6 There is an intriguing parallel, between the glee with which the NSA welcomed, and presumably supported, ‘abstract cryptography’ and the heavy sponsorship of abstract art by the CIA. This support was seen as a useful diversion tactic from more socially engaged art which was considered too sympathetic of communist ideas at the time.

References and Further Reading

Chapter 1

Bennet, J. 2014 '"Literacies" – 60+ Years of "Reading" the Aegean Late Bronze Age', *Bulletin of the Institute of Classical Studies* 57.2: 127–37

Brown, A. 1986 '"I Propose to Begin at Cnossos." John Myres's Visit to Crete in 1893', *Annual of the British School at Athens* 81: 37–44

Cowley, A. E. 1927 'A Note on Minoan Writing', in Casson, E. (ed.) *Essays in Aegean Archaeology Presented to Sir Arthur Evans in Honour of his 75th Birthday*, Oxford, 5–7

Evans, A. J. 1894 'A Mycenaean System of Writing in Crete and the Peloponnese', *The Athenaeum* 3478 (June 23): 812–13

— 1899–1900 'Knossos. Summary Report of the Excavations in 1900: I. The Palace', *Annual of the British School at Athens* 6, 3–70

— 1928 *The Palace of Minos: A comparative account of the successive stages of the early Cretan civilization as illustrated by the discoveries at Knossos*, vol. 2, London

— 1935 *The Palace of Minos: A comparative account of the successive stages of the early Cretan civilization as illustrated by the discoveries at Knossos*, vol. 4, London

— 1936 'Exhibition Illustrative of Minoan Culture with Special Relation to the Discoveries at Knossos Arranged by Sir Arthur Evans in Connexion with the Jubilee of the British School at Athens', in J. L. Myres (ed.), *British Archaeological Discoveries in Greece and Crete 1886–1936: Catalogue of the exhibition*, London, 5–33

Evans, J. 1943 *Time and Chance: The story of Arthur Evans and his forebears*, London

Galanakis, Y. 2014 'Arthur Evans and the Quest for the "Origins of Mycenaean Culture"', in Y. Galanakis, T. Wilkinson and J. Bennet (eds), *ATHYRMATA: Critical essays on the archaeology of the eastern Mediterranean in honour of E. Susan Sherratt*, Oxford, 85–98

— 2015 '"Islanders vs. Mainlanders," "The Mycenae Wars," and Other Short Stories: An archival visit to an old debate', in N. Vogeikoff-Brogan, J. L. Davis and V. Florou (eds), *Carl W. Blegen: Personal and archaeological narratives*, Atlanta, 99–120

Pope, M. 1975 *The Story of Archaeological Decipherment: From Egyptian hieroglyphs to Linear B*, New York and London

Robinson, A. 2002 *The Man Who Deciphered Linear B: The story of Michael Ventris*, New York

Sayce, A. H. 1896 'The beginnings of Aegean Art and Writing', *The Academy* 1269 (August 29): 149-150

Tylor, E. B. 1873 *Primitive Culture: Researches into the development of mythology, philosophy, religion, language, art and custom*, 2nd edn, London

— 1881 *Anthropology: An introduction to the study of man and civilization*, London

Ventris, M. 1952 'Deciphering Europe's Earliest Scripts', *The Listener* 10 July: 57–8

Chapter 2

Bennett, E. L. 1951 *The Pylos Tablets: A preliminary transcription*, Princeton

Briggs, W. 2011 'Emmett L. Bennett Jr. 1918–2011', *Classical Association of the Middle West and South*: https://camws.org/emmett-l-bennett-jr

Chadwick, J. 1992 *The Decipherment of Linear B*, 2nd edn, Cambridge

Davies, W. V. 1987 *Reading the Past: Egyptian hieroglyphs*, London

Evans, A. J. 1935 *The Palace of Minos: A comparative account of the successive stages of the early Cretan civilization as illustrated by the discoveries at*

Knossos, vol. IV:2, London

— 1952 *Scripta Minoa: The written documents of Minoan Crete with special reference to the archives of Knossos*, vol. II, *The Archives of Knossos: Clay tablets inscribed in Linear script B, edited from notes and supplemented by John L. Myres*, Oxford

Fox, M. 2013 *The Riddle of the Labyrinth: The quest to crack an ancient code*, New York

Killen, J. T. and A. Morpurgo Davies 2002 'John Chadwick 1920–1998', *Proceedings of the British Academy* 115: 133–65; available online at http://www.britac.ac.uk/pubs/proc/files/115p133.pdf

Kober, A. E. 1946 'Inflection in Linear Class B: 1 – Declension', *American Journal of Archaeology* 50: 268–76

— 1948 'The Minoan Scripts: Fact and theory', *American Journal of Archaeology* 52: 82–103

Robinson, A. 2002 *The Man Who Deciphered Linear B: The story of Michael Ventris*, London

Ventris, M. 1952 'The Cretan Tablets', BBC Third Programme, 1 July 1952; extract available online at http://www.bbc.co.uk/news/magazine-22799109

— and J. Chadwick 1953 'Evidence for Greek Dialect in the Mycenaean Archives', *Journal of Hellenic Studies* 73: 84–103

— and J. Chadwick 1956/1973 *Documents in Mycenaean Greek*, 1st/2nd edn, Cambridge

— and A. Sacconi (ed.) 1988 *Work-notes on Minoan Language Research and Other Unedited Papers*, Rome

All quoted correspondence is from the collections of the Mycenaean Epigraphy Room, Faculty of Classics, Cambridge; selected letters available at http://www.classics.cam.ac.uk/seminars/projects/mycep/archive/correspondence

Chapter 3

Aruz, J., K. Benzel and J. E. Evans (eds), 2008 *Beyond Babylon: Art, trade, and diplomacy in the second millennium BC*, New York

Bennet, J., 2008 'Palace™: Speculations on palatial production in Mycenaean Greece with (some) reference to glass', in C. M. Jackson and E. C. Wager (eds), *Vitreous Materials in the Late Bronze Age Aegean,* Oxford, 151–72

Blegen, C. W. 1955 'The Palace of Nestor Excavations of 1954', *American Journal of Archaeology* 59: 31–7

Chadwick, J. 1990 *The Decipherment of Linear B*, 2nd edn, Cambridge

Del Freo, M. and M. Perna (eds), 2016 *Manuale di epigrafia micenea: Introduzione allo studio dei testi in lineare B*, vols 1–2, Padua

Duhoux, Y. and A. Morpurgo Davies (eds), 2008–14 *A Companion to Linear B: Mycenaean Greek texts and their world*, vols 1–3, Louvain-la-Neuve and Walpole MA

Feldman, M. H. 2006 *Diplomacy by Design: Luxury arts and an 'international style' in the Ancient Near East, 1400-1200 BCE*, Chicago

Finley, M. I. 1957 'Homer and Mycenae: Property and Tenure', *Historia: Zeitschrift für Alte Geschichte* 6:2: 133–59

Jones, B. R. 2015 *Ariadne's Threads: The construction and significance of clothes in the Aegean Bronze Age*, Leuven and Liège

Halstead, P. 1993 'Lost Sheep? On the Linear B evidence for breeding flocks at Knossos and Pylos', *Minos* 25–26: 343–65

— 1995.'Late Bronze Age Grain Crops and Linear B Ideograms *65, *120, and *121', *Annual of the British School at Athens* 90: 229–34

Haskell, H. W., R. E. Jones, P. M. Day and J. T. Killen, 2011 *Transport Stirrup Jars of the Bronze Age Aegean and East Mediterranean*, Philadelphia

Judson, A. P. 2013 'The Linear B Inscribed Stirrup Jars', *Kadmos* 52: 69–110

Killen, J. T., 1964 'The Wool Industry of Crete in the Late Bronze Age', *Annual of the British School at Athens* 59: 1–15

McArthur, J. K. 1993 *Place-names in the Knossos Tablets: Identification and location*, Salamanca

Nakassis, D. 2013 *Individuals and Society in Mycenaean Pylos*, Leiden and Boston

Nosch, M.-L. 2014 'Mycenaean Wool Economies in the Latter Part of the 2nd Millennium BC Aegean', in C. Breniquet and C. Michel (eds), *Wool Economy in the Ancient Near East and the Aegean: From the beginnings of sheep husbandry to institutional textile industry*, Oxford, 371–400

Postgate, J. N. 2013 *Bronze Age Bureaucracy: Writing and the practice of government in Assyria*, Cambridge

Van de Mieroop, M., 2007 *The Eastern Mediterranean in the Age of Ramesses II*, Oxford

Wright, J. C. (ed.), 2004 *The Mycenaean Feast*, Princeton

Chapter 4

Evans, A. J. 1909 *Scripta Minoa: The written documents of Minoan Crete with special reference to the archives of Knossos*, vol. 1., *The Hieroglyphic and Primitive*

Linear Classes: With an account of the discovery of the Pre-Phoenician Scripts, their place in Minoan story and their Mediterranean relations, Oxford

Ferrara, S. 2012–13 *Cypro-Minoan Inscriptions,* vol. 1, *Analysis*, vol. 2, *Corpus*, Oxford

Godart, L. and J.-P. Olivier 1976–85 *Recueil des inscriptions en Linéaire A*, vols 1–5, *Études Crétoises* 21.1–5, Paris

Steele, P. M. 2013 *A Linguistic History of Ancient Cyprus: The non-Greek languages, and their relations with Greek, c. 1600–300 BC*, Cambridge

— (ed.) 2017 *Understanding Relations Between Scripts: The Aegean writing systems*, Oxford

Find out more about the project *Contexts of and Relations between Early Writing Systems* (CREWS) online at https://crewsproject.wordpress.com/

Chapter 5

Aurora, F. 2015 'DĀMOS (Database of Mycenaean at Oslo): Annotating a fragmentarily attested language', *Procedia – Social and Behavioral Sciences* 198: 21–31 (available at http://dx.doi.org/10.1016/j.sbspro.2015.07.415)

Del Freo M. and F. Di Filippo 2014 'LiBER: un progetto di digitalizzazione dei testi in scrittura lineare B', *Archeologia e Calcolatori* 25: 33–50 (available at http://www.archcalc.cnr.it/indice/PDF25/02_Del_Freo_Di_Filippo.pdf)

Mahony, S. and G. Bodard (eds) 2010 *Digital Research in the Study of Classical Antiquity*, London

Nakassis, D. forthcoming 'Vorsprung durch Technik: Imaging the Linear B tablets from Pylos', in M. L. Nosch, H. Landenius Enegren (eds), *Proceedings of the 14th Mycenological Colloquium, Copenhagen, 2–5 September 2015*, Rome

Snyder, B., R. Barzilay and K. Knight, 2010 'A Statistical Model for Lost Language Decipherment', *ACL 2010, Proceedings of the 48th Annual Meeting of the Association for Computational Linguistics, July 11–16, 2010*, Uppsala, 1048–57 (available at http://delivery.acm.org/10.1145/1860000/1858788/p1048-snyder.pdf]

Chapter 6

Andrew, C. 1985 'F. H. Hinsley and the Cambridge Moles: Two patterns of intelligence recruitment', in R. Langhorne (ed.), *Diplomacy and Intelligence During the Second World War,* Cambridge, 22–40

Batey, M. 2009 *Dilly: The man who broke enigmas,* London

Burman, A. 2013 *Gendering Decryption – Decrypting Gender: The gender discourse of labour at Bletchley Park 1939–1945,* MA dissertation, Uppsala University (available at http://www.diva-portal.org/smash/get/diva2:625771/FULLTEXT01.pdf)

Chadwick, J. 1958 *The Decipherment of Linear B,* Cambridge

— unpublished *Memoirs: Unpublished memoirs in the collections of the Mycenaean Epigraphy Group,* Faculty of Classics, University of Cambridge

Erskine, R. and M. Smith (eds), 2011 *The Bletchley Park Codebreakers,* London

Hodges, A. 1992 *Alan Turing: The enigma*, London

Hunter, E. 2003 'A View of "The Park" (minimizing contravention of the Official Secrets Act)', in M. Smith (ed.), *Other People's Stories Book 6*, Bletchley Park, 5–9

Lee, J. A. N. and G. Holtzman 1995 '50 Years after Breaking the Codes: Interviews with two of the Bletchley Park scientists', in *IEEE Annals of the History of Computing* 17: 32–43

McKay, S. 2013 *The Lost World of Bletchley Park: An illustrated history of the wartime codebreaking centre*, London

Richmond, J. 2001 'Classics and Intelligence: Part I', in *Classics Ireland* 8: 84–101

Singh, S. 2000 *The Code Book: The secret history of code and code-breaking,* London

Smith, M. 2011 *The Secrets of Station X: How the Bletchley Park codebreakers helped win the war,* London

Wilkinson, P. 2001 'Italian Naval Decrypts', in Hinsley, F. H. and A. Stripp (eds), *Codebreakers: The Inside Story of Bletchley Park*, Oxford, 61–7

Chapter 7

Aleph One 1996 'Smashing the Stack for Fun and Profit', *Phrack* 49 (14), http://phrack.org/issues/49/14.html.

Clark, D. 1988 'The Design Philosophy of the Darpa Internet Protocols', *SIGCOMM Comput. Commun. Rev.* 18(4), New York, ACM, 106–14 doi:10.1145/52325.52336

Diffie, W., and M. Hellman, 1976 'New Directions in Cryptography', *IEEE Transactions on Information Theory* 22(6), 644–54, doi:10.1109/TIT.1976.1055638

Ellis, J, 1969 'The Possibility of Secure Non-Secret Encryption', CESG Research Report no. 3006, Cheltenham, GCHQ, https://www.gchq.gov.uk/possibility-secure-non-secret-encryption

Guri, M., A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky and Y. Elovici, 2015 'GSMem: Data Exfiltration from Air-Gapped Computers over Gsm Frequencies', in 24th Usenix Security Symposium (Usenix Security 15), 849–64, Washington, https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/guri

Hastings, M., 2016 *The Secret War: Spies, Ciphers, and Guerrillas 1939–1945*, New York

Rivest, R. L., A. Shamir, and L. Adleman, 1978 'A Method for Obtaining Digital Signatures and Public-Key Cryptosystems', *Communications of the ACM* 21(2), New York, 120–6, doi:10.1145/359340.359342

Szekeres, L., M. Payer, T. Wei and D. Song, 2013 'SoK: Eternal War in Memory', in *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, 48–62, SP '13, Washington, doi:10.1109/SP.2013.13

Chapter 8

Copeland, B. J. (ed.), 2004 *The Essential Turing*, Oxford

Hodges, A., 1983 *Alan Turing: The enigma*, New York

Petzold, C., 2008 *The Annotated Turing: A guided tour through Alan Turing's historic paper on computability and the Turing machine,* Indianapolis

Rejewski, M., 1980 'An Application of the Theory of Permutations in Breaking the Enigma Cipher', *Applicationes mathematicae* 16 (4)

Singh, S., 1999 *The Code Book: The evolution of secrecy from Mary, Queen of Scots, to quantum cryptography*, New York

Welchman, G, 1982 *The Hut Six Story: Breaking the Enigma codes*, New York

Chapter 9

Bauer, F. L. 2006 'The Tiltman Break', in Copeland et al. 2010, appendix 5

Copeland, B. J. et al. 2010 *Colossus: The Secrets of zBletchley Park's Codebreaking Computers* (2nd edn), Oxford

Clabby, John, 2007, *Brigadier John Tiltman A Giant Among Cryptanalysts* Fort Meade MD www.nsa.gov

Davies, D. 1995 'The Lorenz Cipher Machine SZ42', *Cryptologia*, vol. 19, pp. 517–39

Hobbs A. M. and Oxley J. G., 2004, 'William T. Tutte', *Notices of the American Mathematical Society* 51.3: 320–30

Tutte, W. T. 1998, *Graph Theory as I Have Known It*, Oxford Lecture Series in Mathematics and its Applications

— 2006 'My Work at Bletchley Park', in Copeland et al. 2010, pp. 352–69

Younger, D. H. 2012, 'William Thomas Tutte, 14 May 1917–2 May 2002,' *Biographical Memoirs of Fellows of the Royal Society* 58: 283–97

Flowers, T. H. 1983 'The Design of Colossus', *Annals of the History of Computing*, 5: 239–52

— 2006 'D-Day at Bletchley Park', in Copeland et al. 2010, pp. 78–83

Chapter 10

Diffie, W. and M. Hellman 1976 'New directions in cryptography', *IEEE Transactions on Information Theory* 22.6: 644–54

Abelson, H., R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller and B. Schneier 1997 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption', *World Wide Web Journal,* Special issue: Web security: a matter of trust archive, 2.3: 241–57

Morris, F. L. and C. B. Jones 1984 'An Early Program Proof by Alan Turing', *IEEE Annals of the History of Computing* 6.2: 139–43 (DOI http://dx.doi.org/10.1109/MAHC.1984.10017)

National Security Agency *Cryptolog Technical Journal*, https://archive.org/details/nsacryptolog

Vryonis, P. 2013 https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5

Index

Numbers in italics refer to illustrations in the text

Knossos continued

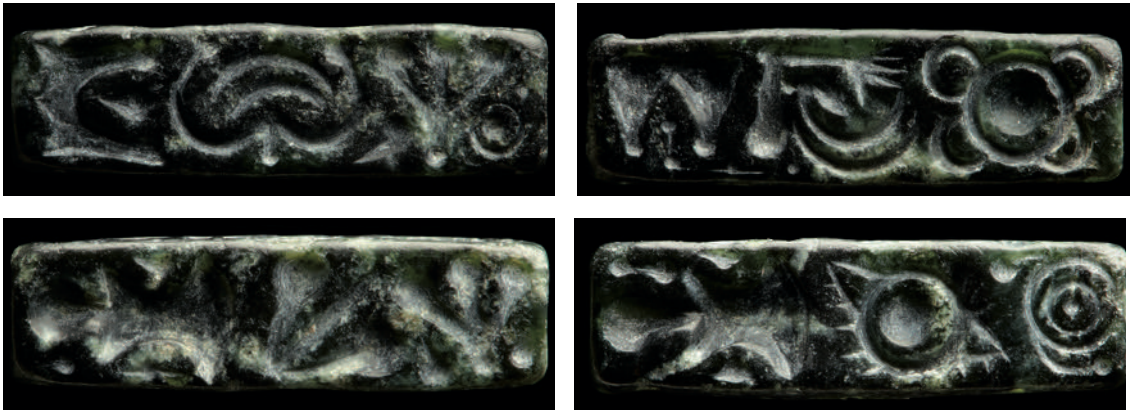


Plate 1 Four-sided seal inscribed in Cretan Hieroglyphic (Courtesy of the Ashmolean Museum, University of Oxford)

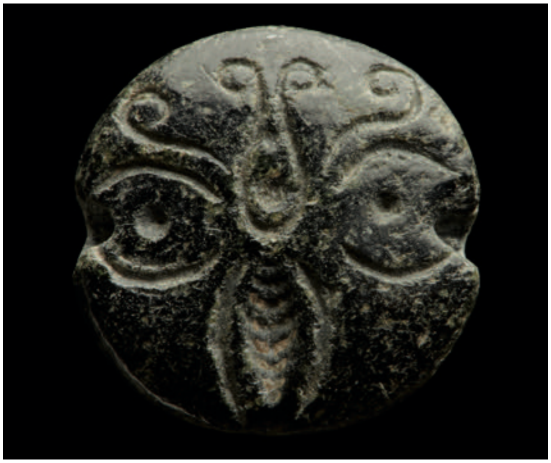


Plate 2 Seal showing a butterfly, bought by Arthur Evans at Makryteichos near Knossos in 1894 (Courtesy of the Ashmolean Museum, University of Oxford)

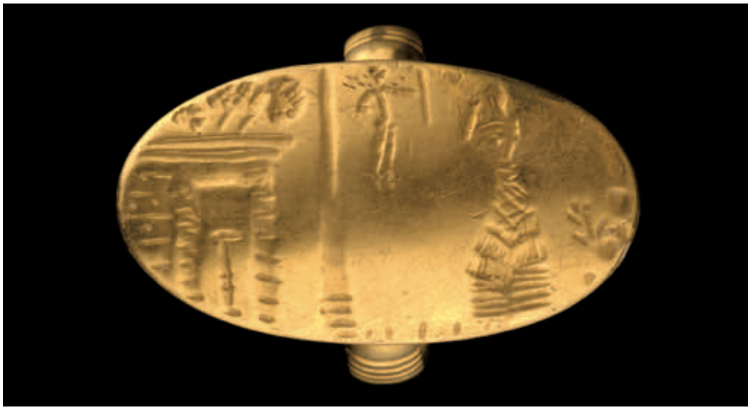


Plate 3 Gold signet ring with a 'scene of worship', said to come from Knossos, bought by Arthur Evans at Herakleion in 1894 (Courtesy of the Ashmolean Museum, University of Oxford)

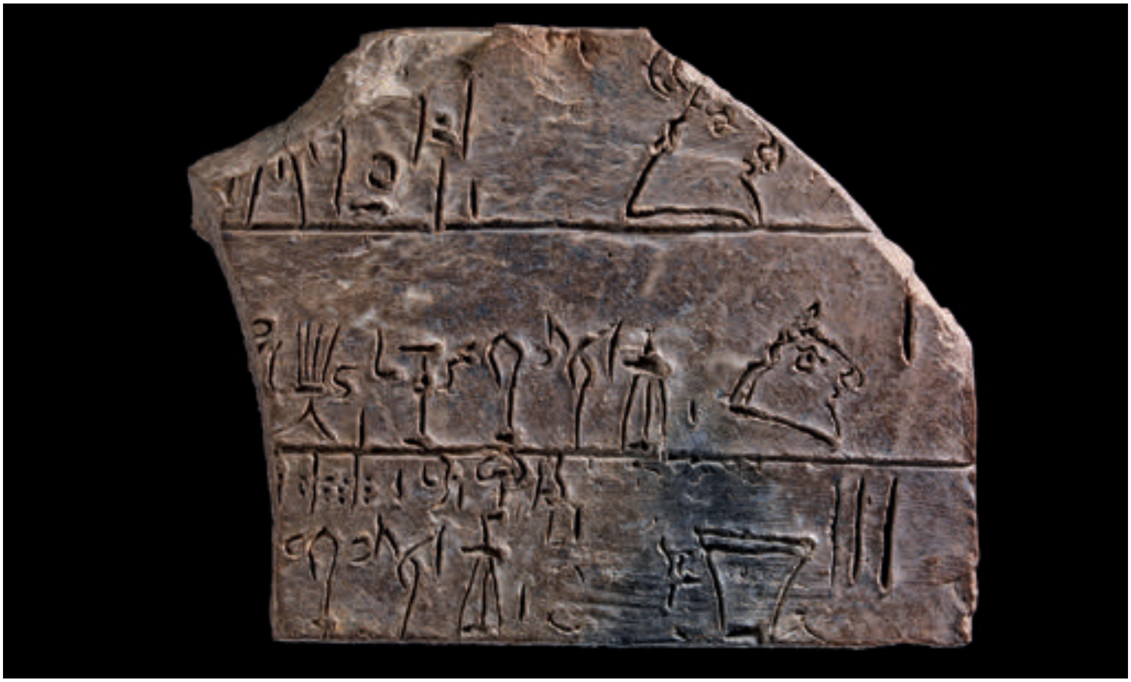


Plate 4 Partially preserved clay tablet from the palace at Knossos recording ritual and drinking vessels in the shape of a bull's head and of handled cups (Courtesy of the Ashmolean Museum, University of Oxford)

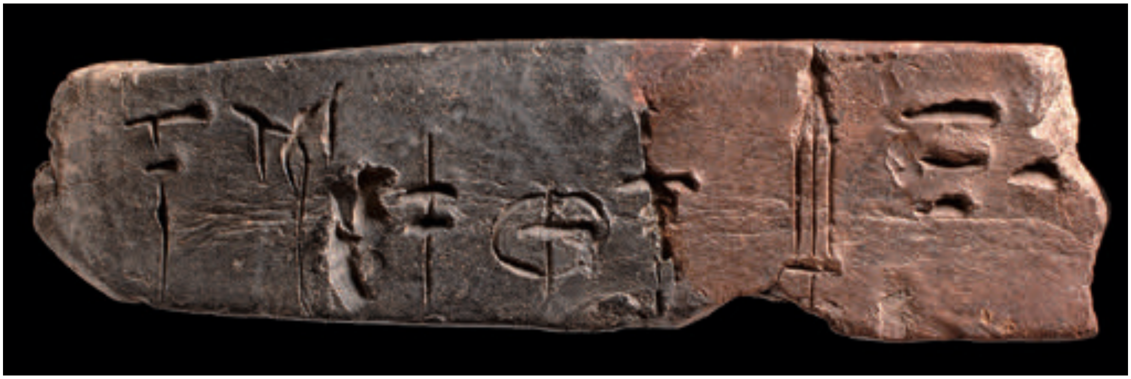


Plate 5 Partially preserved Linear B tablet from the palace at Knossos recording short swords, 'pa-ka-na' (Courtesy of the Ashmolean Museum, University of Oxford)

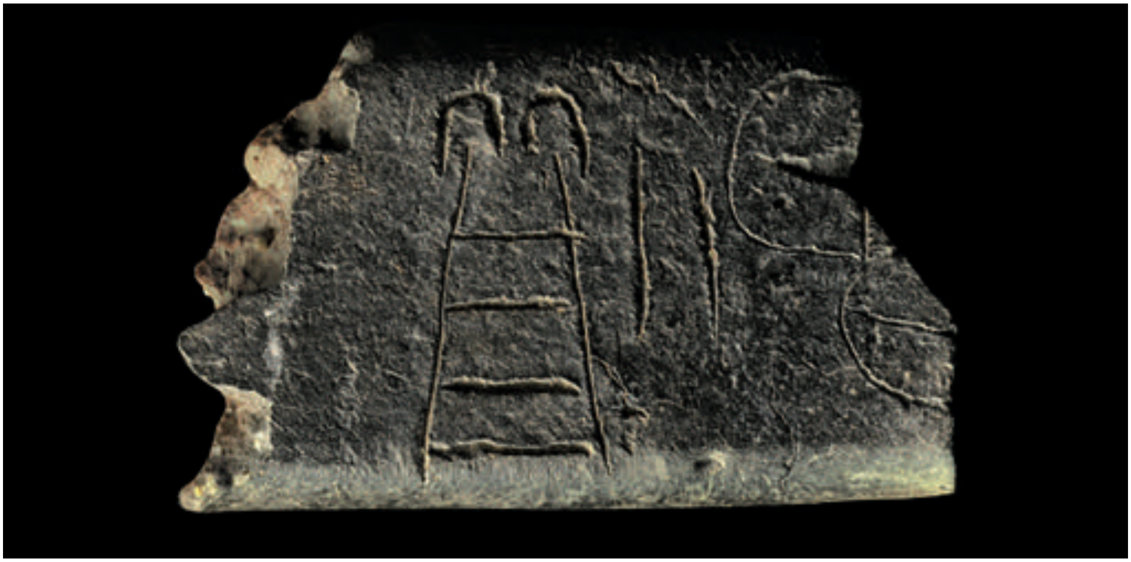


Plate 6 Fragment of a Linear B tablet from the palace at Knossos recording two body armours and a wheeled chariot (the latter only partly visible) (Courtesy of the Ashmolean Museum, University of Oxford)

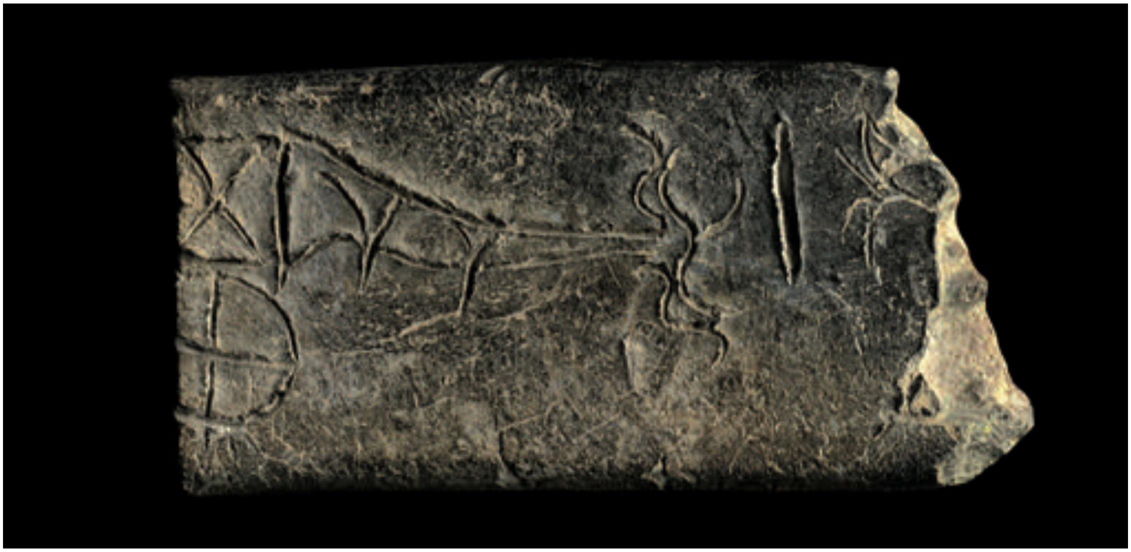


Plate 7 Fragment of a Linear B tablet from the palace at Knossos recording one wheeled chariot and a horse (the latter only partly visible) (Courtesy of the Ashmolean Museum, University of Oxford)

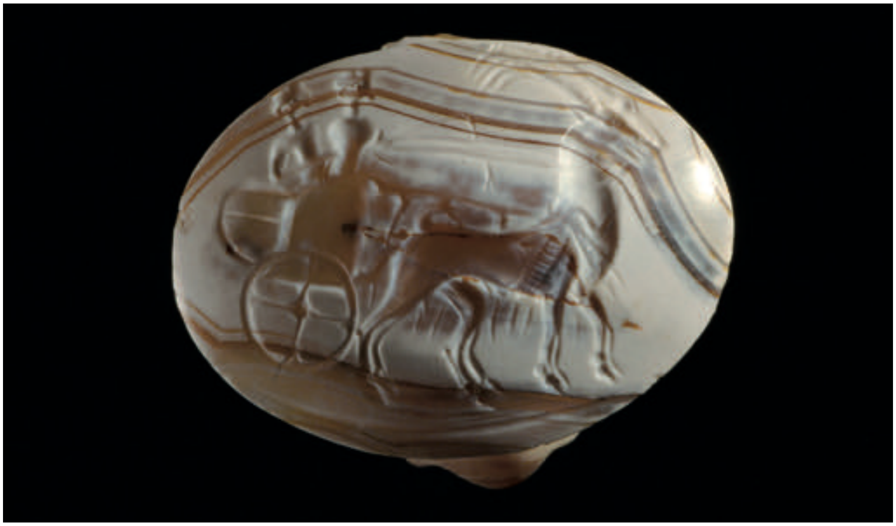


Plate 8 Signet ring engraved with two figures driving a chariot drawn by Cretan wild goats (Courtesy of the Ashmolean Museum, University of Oxford)

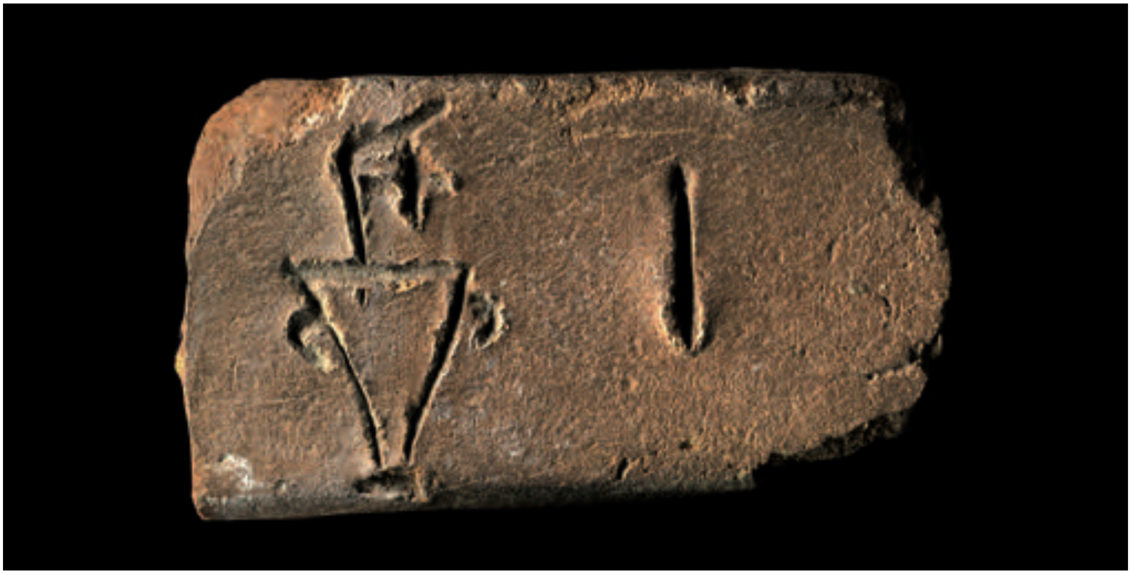


Plate 9 Fragment of a Linear B tablet recording a water jug from Knossos (Courtesy of the Ashmolean Museum, University of Oxford)

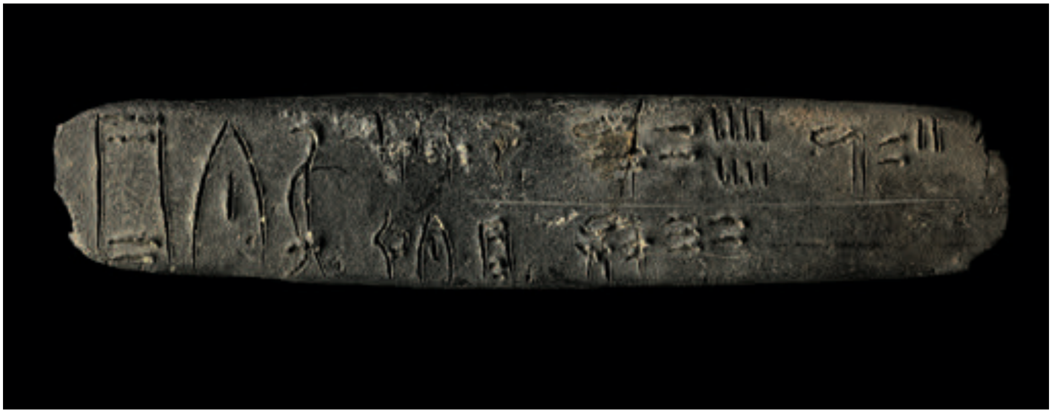


Plate 10 Complete Linear B tablet from the palace at Knossos recording sheep at a place called 'da-ti-jo' (Courtesy of the Ashmolean Museum, University of Oxford)

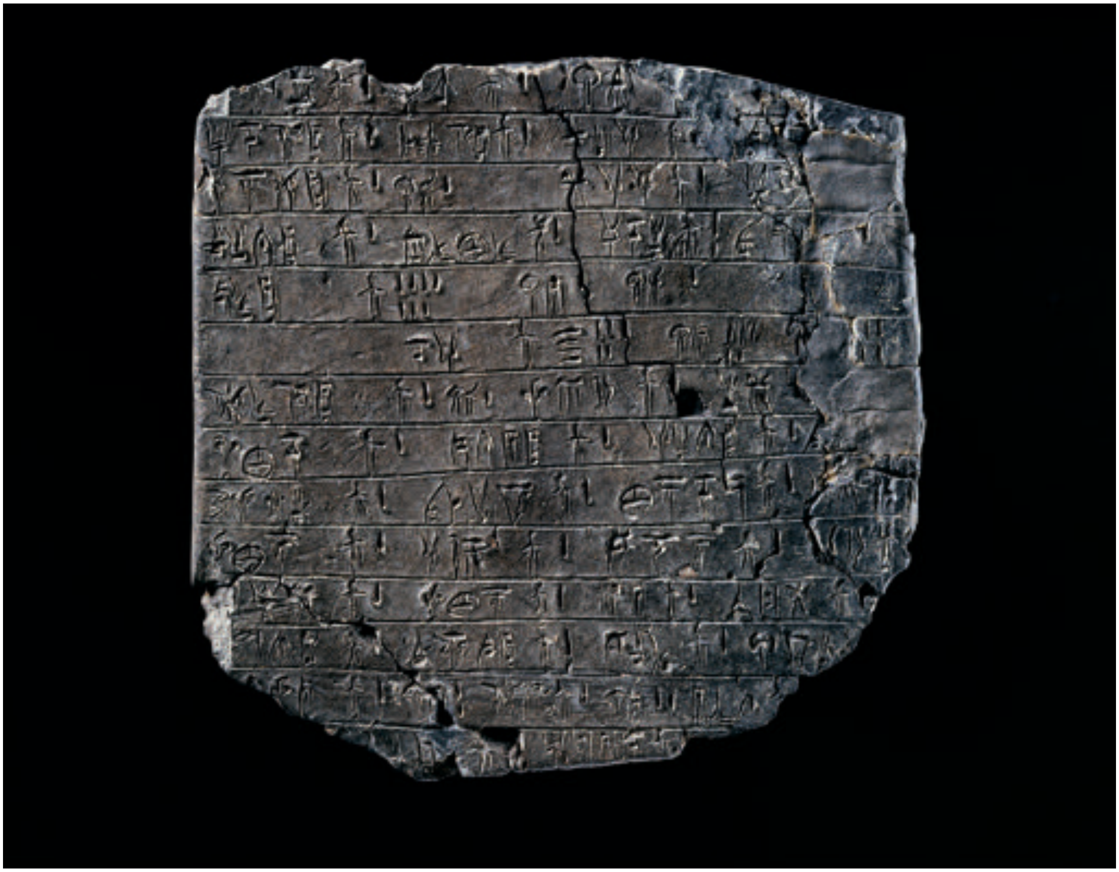


Plate 10 Page-shaped Linear B tablet, partially preserved, from the palace at Knossos. It records women workers accompanied by 'girls' and 'boys' (Courtesy of the Ashmolean Museum, University of Oxford)

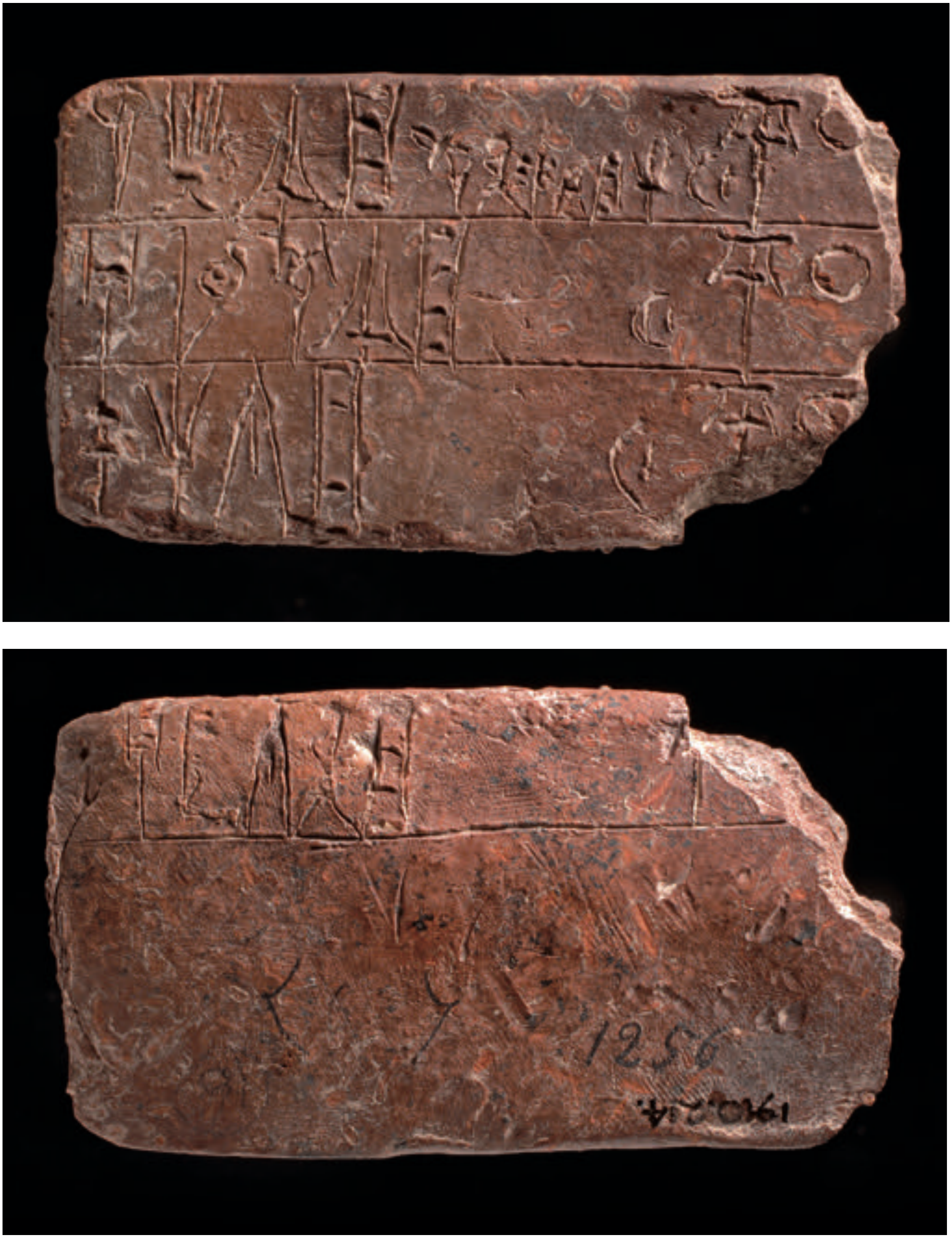


Plate 12 Partially preserved Linear B tablet from the Palace at Knossos recording the allocation of rations to women (Courtesy of the Ashmolean Museum, University of Oxford)

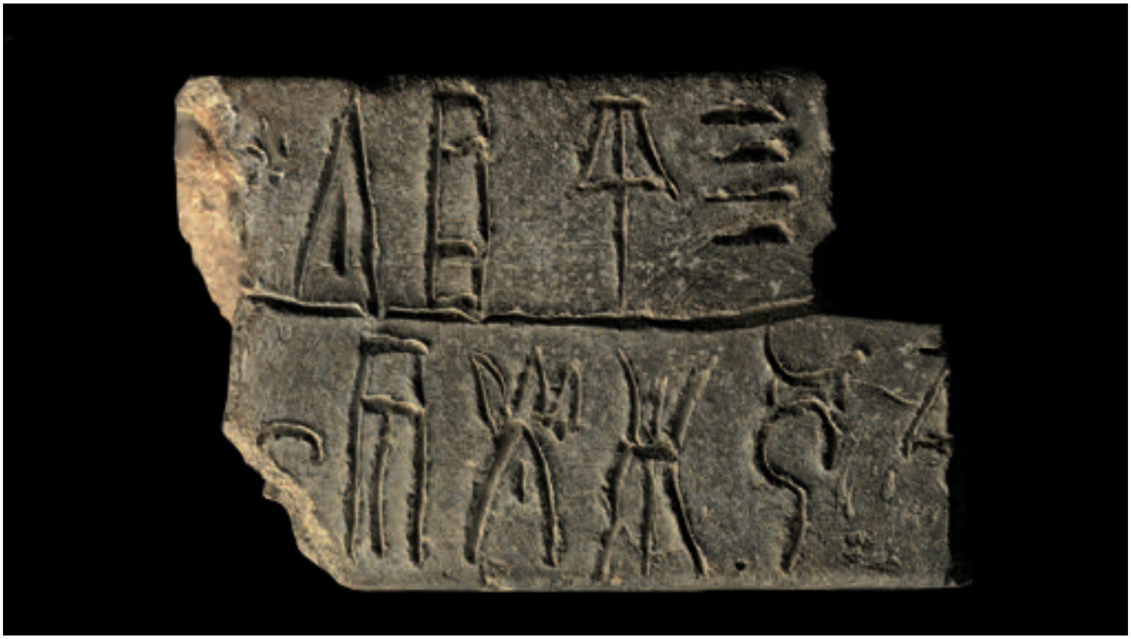


Plate 13 Fragment of a Linear B tablet recording plots of land measured in 'seed' grain' (see also p. 41) from the Herakleion Museum in Crete (Courtesy of the Ashmolean Museum, University of Oxford)

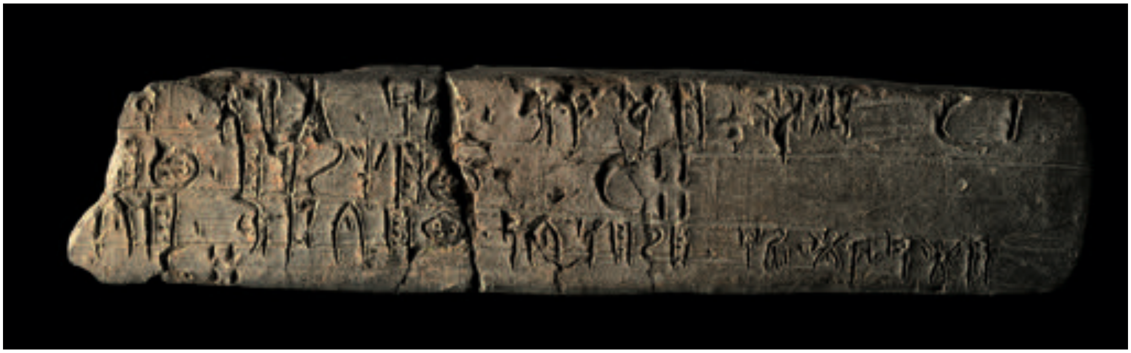


Plate 14 Partially preserved Linear B tablet from the palace at Knossos, most likely recording rations of barley, 'ki-ri-ta', to groups of women, one coming from Chania in west Crete, recorded as 'ku-do-ni-ja' in the top line (Courtesy of the Ashmolean Museum, University of Oxford)

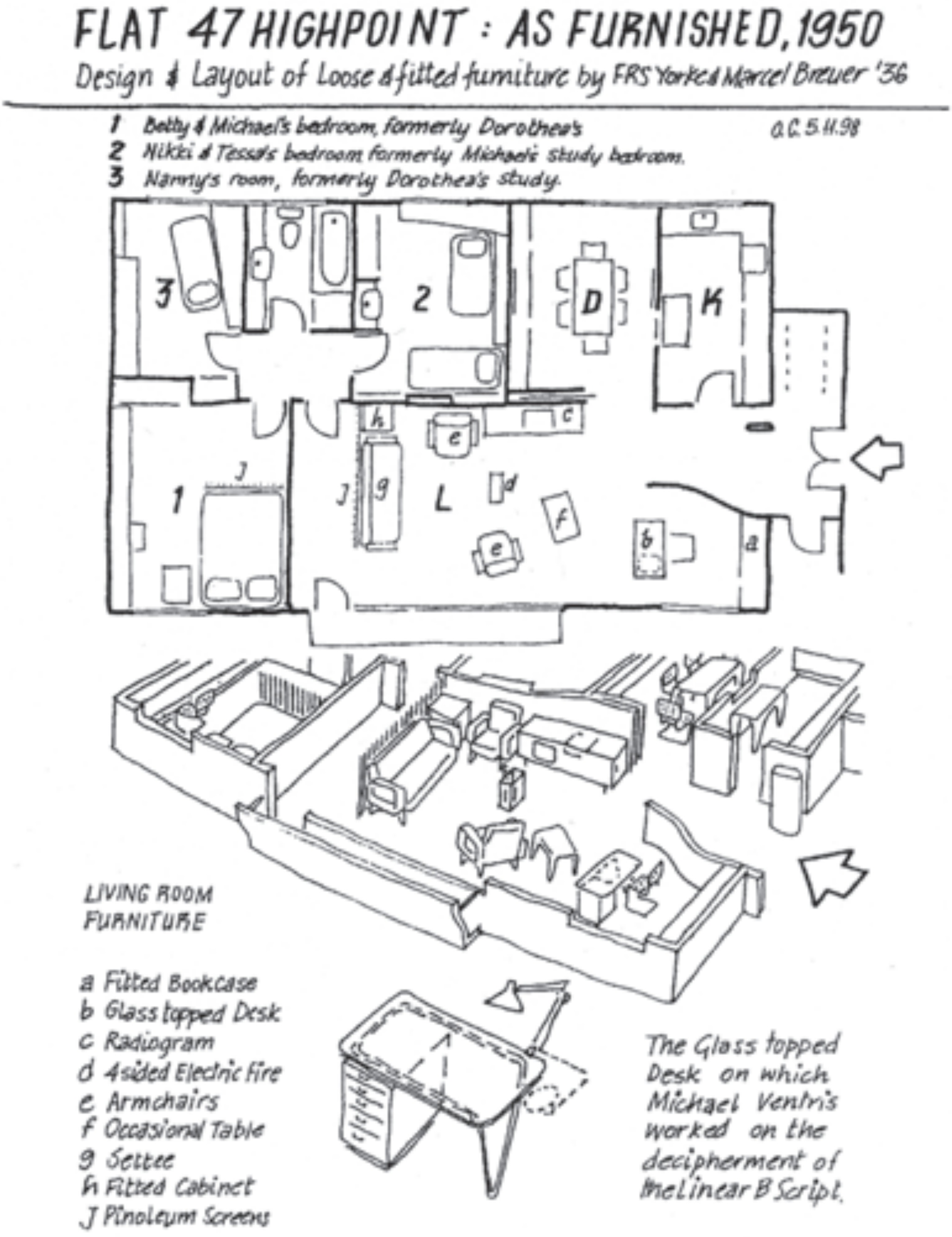

FLAT 47 HIGHPOINT : AS FURNISHED, 1950
Design & Layout of Loose & fitted furniture by FRS Yorke & Marcel Breuer '36
1 Betty & Michael's bedroom, formerly Dorothea's
2 Nikki & Tessa's bedroom formerly Michael's study bedroom.
3 Nanny's room, formerly Dorothea's study.
O.C. 5.11.98
3
2
D
K
1
J
J
g
L
h
e
c
d
f
e
b
a
LIVING ROOM FURNITURE
a Fitted Bookcase
b Glass topped Desk
c Radiogram
d 4sided Electric Fire
e Armchairs
f Occasional Table
g Settee
h Fitted Cabinet
J Pinoleum Screens
The Glass topped Desk on which Michael Ventris worked on the decipherment of theLinear B Script.

Plate 15 A sketch by Oliver Cox of 47 Highpoint, the home of Michael Ventris and his family. Among other pieces of furniture, we see in the living room the location of Breuer's glass-topped desk on which Ventris worked on the decipherment of Linear B. Courtesy of Andrew Robinson (from his book 'The Man Who Deciphered Linear B: The Story of Michael Ventris' 2002, London, p. 77).

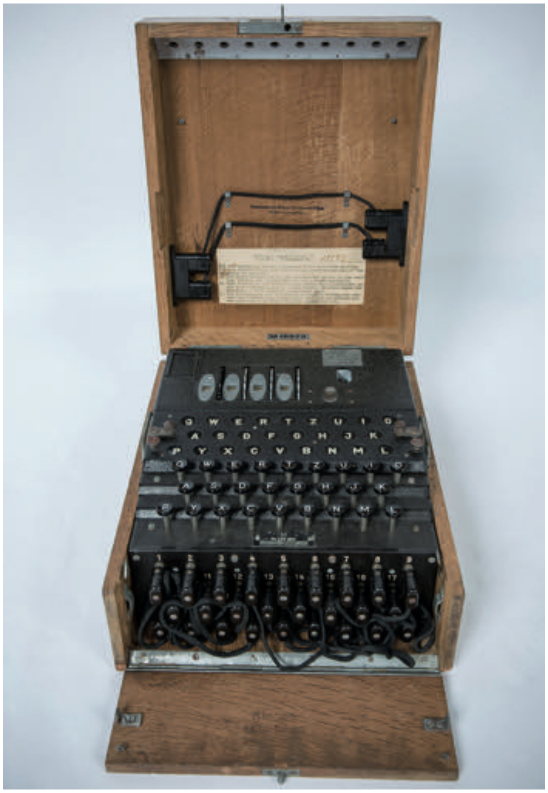


Plate 16 The Enigma Machine (Crown Copyright 2017)

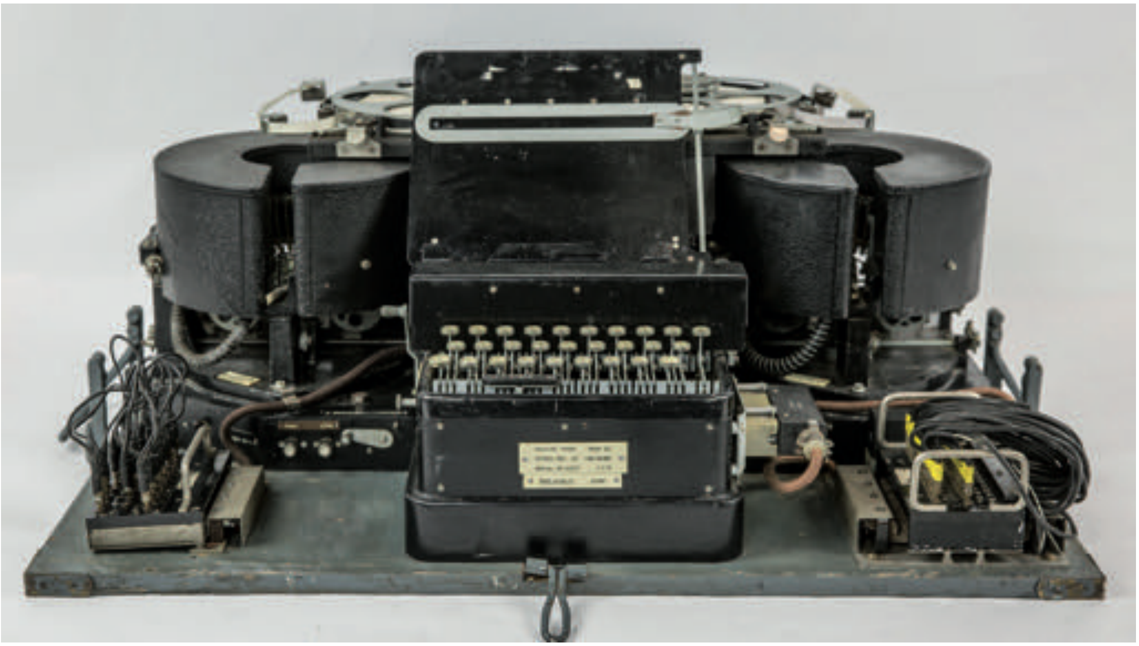
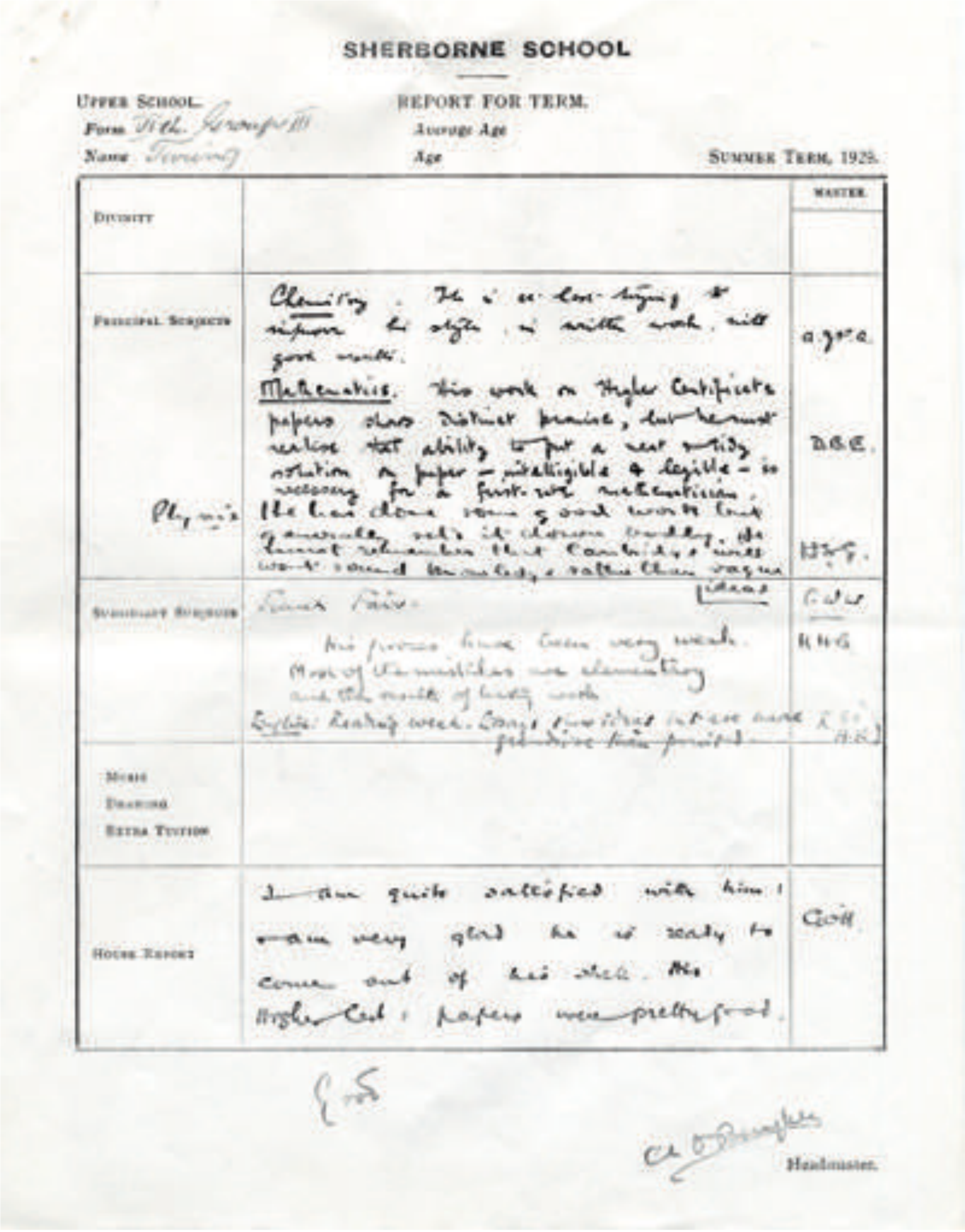


Plate 17 The Typex machine (Crown Copyright 2017)

Plate 18 Alan Turing sitting on the porch of his family house (Courtesy of King's College Library, Cambridge)



SHERBORNE SCHOOL

UPPER SCHOOL. REPORT FOR TERM.

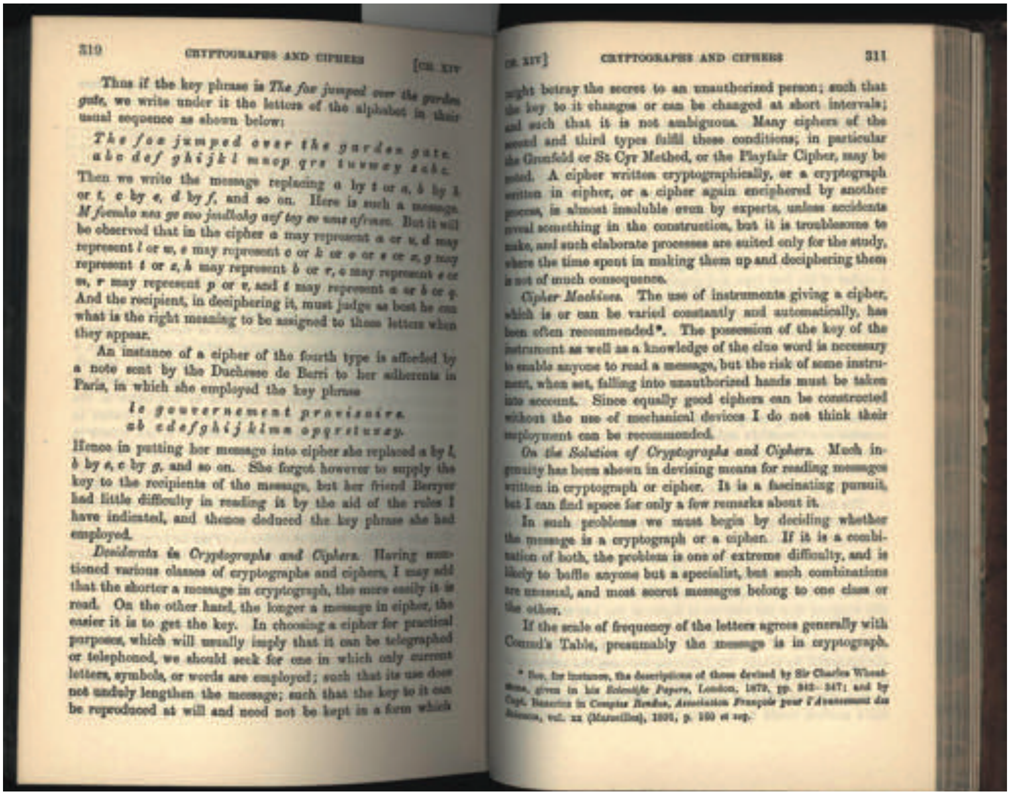
Form VIth. Group III Average Age

Name Turing Age SUMMER TERM, 1929.

DIVINITY		MASTER.
PRINCIPAL SUBJECTS	Chemistry. He is [illegible] & inferior in style in written work, with good results. Mathematics. His work on Higher Certificate papers shows distinct promise, but he must realise that ability to put a neat & tidy solution on paper — intelligible & legible — is necessary for a first-rate mathematician. Physics He has done some good work but generally sets it down badly. He must remember that Cambridge will want sound knowledge rather than vague ideas	a.g.e. D.B.E. H.R.G.
SUBSIDIARY SUBJECTS	French Prose. His proses have been very weak. Most of the mistakes are elementary and the result of hasty work. English: Reading weak. Essays show ideas but are more [illegible] than finished.	G.H.W. H.H.G. [illegible]
MUSIC DRAWING EXTRA TUITION		
HOUSE REPORT	I am quite satisfied with him & am very glad he is ready to come out of his shell. His Higher Cert. papers were pretty good.	G.O.H.

C. L. F. Boughey
Headmaster.

Plate 19 A report from Sherborne, Alan Turing's school where he is stated as a first-class mathematician (Courtesy of Sherbourne School and King's College Library, Cambridge)



310 CRYPTOGRAPHS AND CIPHERS [CH. XIV

Thus if the key phrase is *The fox jumped over the garden gate*, we write under it the letters of the alphabet in their usual sequence as shown below:

The fox jumped over the garden gate.
abc def ghijkl mnop qrs tuvwxy zabc.

Then we write the message replacing *a* by *t* or *a*, *b* by *h* or *t*, *c* by *e*, *d* by *f*, and so on. Here is such a message. *M foemlo nea ge eoo jesdlohg aef teg ee uase afraae.* But it will be observed that in the cipher *a* may represent *a* or *u*, *d* may represent *l* or *w*, *e* may represent *c* or *k* or *o* or *s* or *x*, *g* may represent *t* or *z*, *h* may represent *b* or *r*, *o* may represent *e* or *m*, *r* may represent *p* or *v*, and *t* may represent *a* or *b* or *q*. And the recipient, in deciphering it, must judge as best he can what is the right meaning to be assigned to those letters when they appear.

An instance of a cipher of the fourth type is afforded by a note sent by the Duchesse de Berri to her adherents in Paris, in which she employed the key phrase

le gouvernement provisoire.
ab cdefghijklmn opqrstuvxy.

Hence in putting her message into cipher she replaced *a* by *l*, *b* by *e*, *c* by *g*, and so on. She forgot however to supply the key to the recipients of the message, but her friend Berryer had little difficulty in reading it by the aid of the rules I have indicated, and thence deduced the key phrase she had employed.

Desiderata in Cryptographs and Ciphers. Having mentioned various classes of cryptographs and ciphers, I may add that the shorter a message in cryptograph, the more easily it is read. On the other hand, the longer a message in cipher, the easier it is to get the key. In choosing a cipher for practical purposes, which will usually imply that it can be telegraphed or telephoned, we should seek for one in which only current letters, symbols, or words are employed; such that its use does not unduly lengthen the message; such that the key to it can be reproduced at will and need not be kept in a form which

CH. XIV] CRYPTOGRAPHS AND CIPHERS 311

might betray the secret to an unauthorized person; such that the key to it changes or can be changed at short intervals; and such that it is not ambiguous. Many ciphers of the second and third types fulfil these conditions; in particular the Grenfeld or St Cyr Method, or the Playfair Cipher, may be noted. A cipher written cryptographically, or a cryptograph written in cipher, or a cipher again enciphered by another process, is almost insoluble even by experts, unless accidents reveal something in the construction, but it is troublesome to make, and such elaborate processes are suited only for the study, where the time spent in making them up and deciphering them is not of much consequence.

Cipher Machines. The use of instruments giving a cipher, which is or can be varied constantly and automatically, has been often recommended*. The possession of the key of the instrument as well as a knowledge of the clue word is necessary to enable anyone to read a message, but the risk of some instrument, when set, falling into unauthorized hands must be taken into account. Since equally good ciphers can be constructed without the use of mechanical devices I do not think their employment can be recommended.

On the Solution of Cryptographs and Ciphers. Much ingenuity has been shown in devising means for reading messages written in cryptograph or cipher. It is a fascinating pursuit, but I can find space for only a few remarks about it.

In such problems we must begin by deciding whether the message is a cryptograph or a cipher. If it is a combination of both, the problem is one of extreme difficulty, and is likely to baffle anyone but a specialist, but such combinations are unusual, and most secret messages belong to one class or the other.

If the scale of frequency of the letters agrees generally with Conrad's Table, presumably the message is in cryptograph.

* See, for instance, the descriptions of those devised by Sir Charles Wheatstone, given in his *Scientific Papers*, London, 1879, pp. 342–347; and by Capt. Bazeries in *Comptes Rendus, Association Française pour l'Avancement des Sciences*, vol. xx (Marseilles), 1891, p. 160 *et seq.*

Plate 20 'Mathematical recreations' by William W. Rouse Ball given to Alan Turing as a prize (Courtesy of King's College Library, Cambridge)

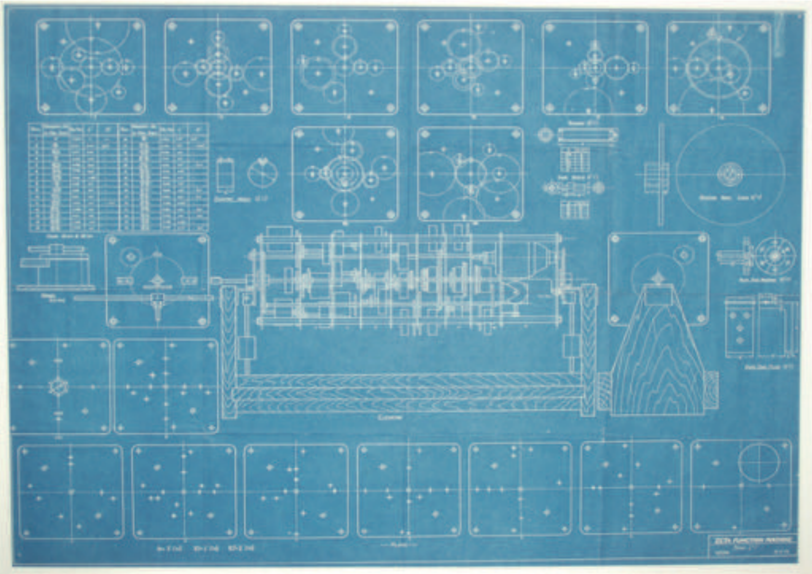
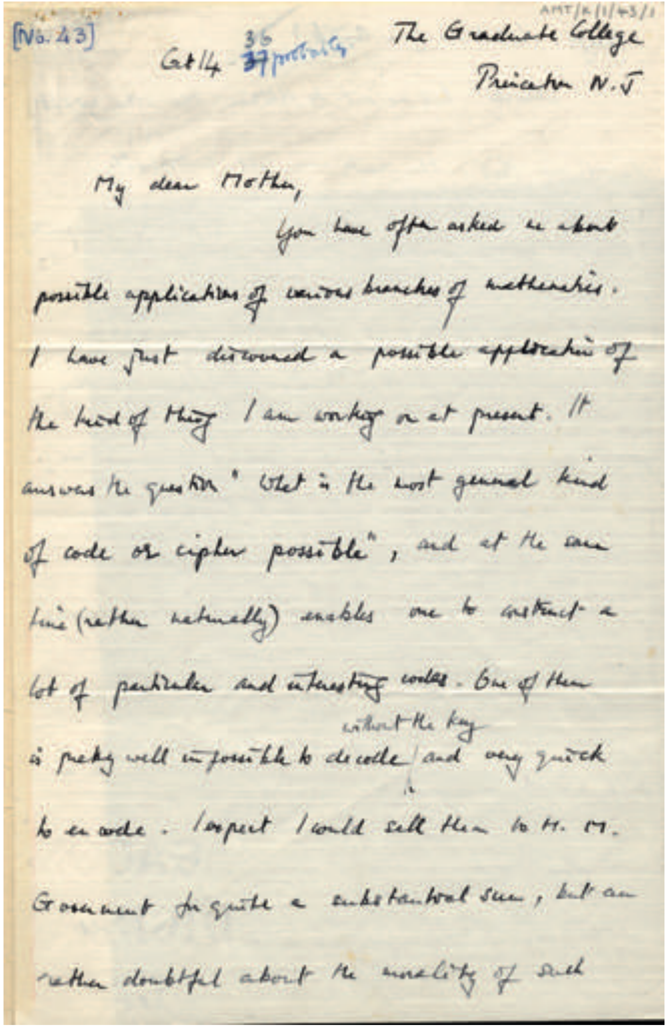


Plate 21 The blueprint for Turing's Zeta Function Machine (Reproduced by kind permission of King's College Library, AMT/C/2, and Mrs Emma McPhail)



AMT/K/1/43/1

[No. 43]

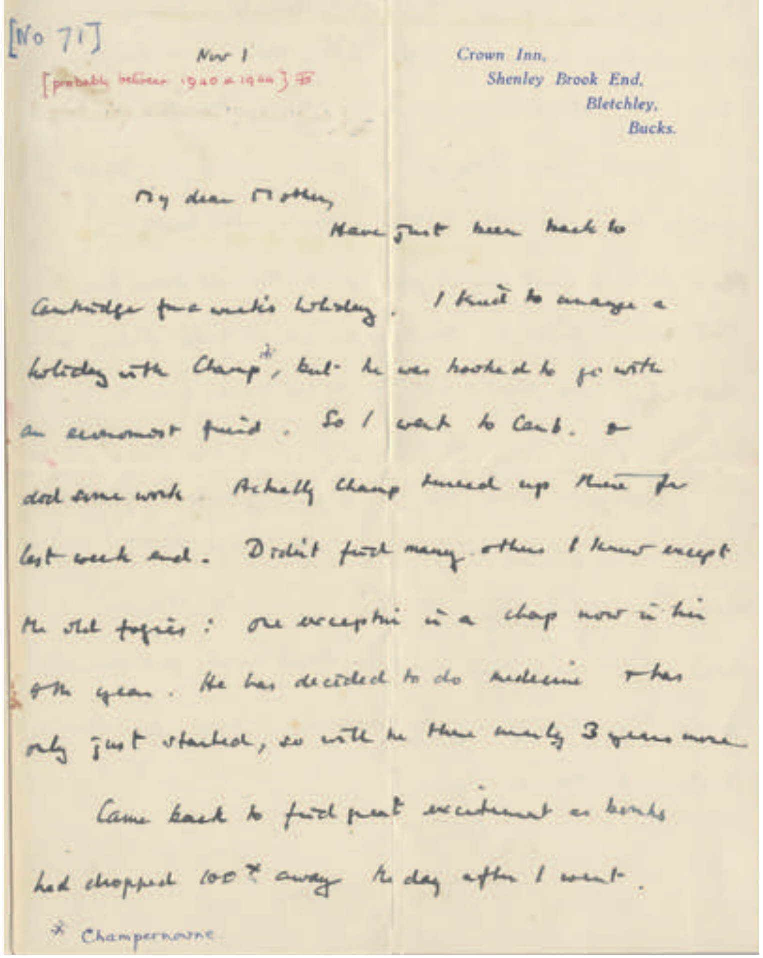
Oct 14 ~~37~~ 36 probably

The Graduate College
Princeton N.J

My dear Mother,

You have often asked me about possible applications of various branches of mathematics. I have just discovered a possible application of the kind of thing I am working on at present. It answers the question 'What is the most general kind of code or cipher possible', and at the same time (rather naturally) enables me to construct a lot of particular and interesting codes. One of them is pretty well impossible to decode without the key and very quick to encode. I expect I could sell them to H. M. Government for quite a substantial sum, but am rather doubtful about the morality of such

Plate 22 A letter of Alan Turing addressed to his mother Sarah Turing written in October 1936 (Courtesy of King's College Library, Cambridge)



[No 71]

Nov 1

[probably between 1940 & 1944] JT

Crown Inn.
Shenley Brook End.
Bletchley.
Bucks.

My dear Mother,

Have just been back to Cambridge for a week's holiday. I tried to arrange a holiday with Champ*, but he was booked to go with an economist friend. So I went to Camb. & did some work. Actually Champ turned up there for last week end. Didn't find many others I knew except the old fogies: one exception is a chap now in his 6th year. He has decided to do medicine & has only just started, so will be there nearly 3 years more.

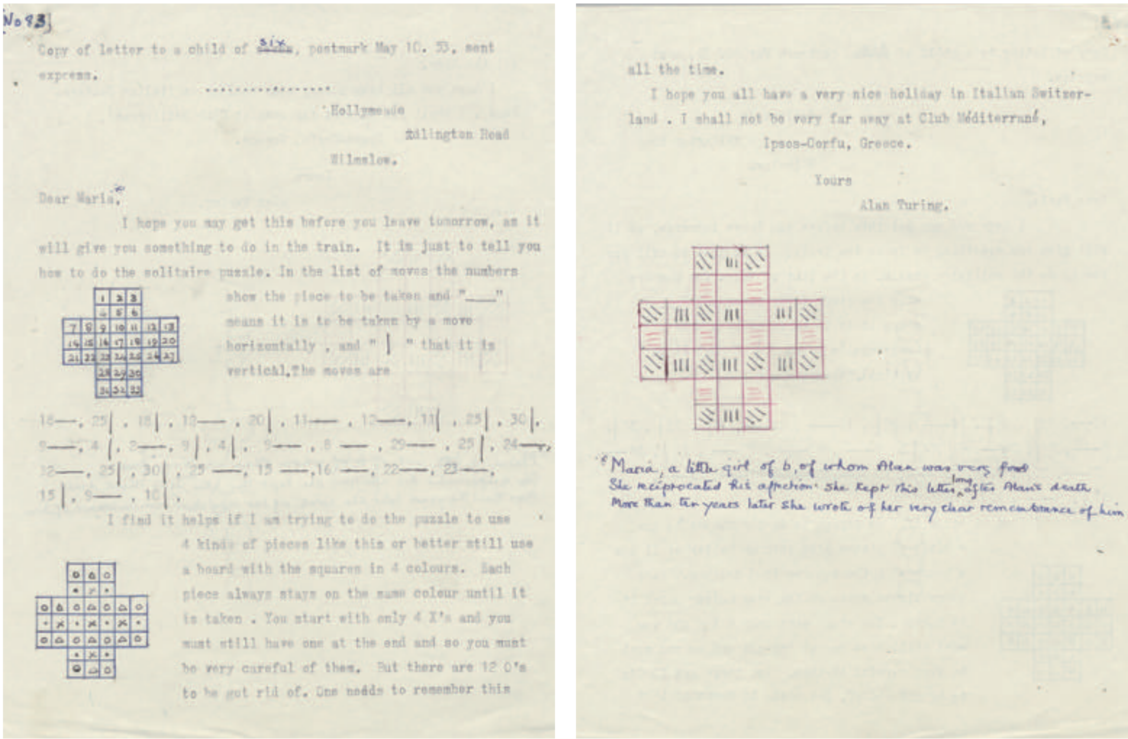
Came back to find great excitement as bombs had dropped 100^{x} away the day after I went.

* Champernowne

Plate 23 A letter of Alan Turing to his mother, from Bletchley (Courtesy of King's College Library, Cambridge)

Plate 24 Alan Turing at Bosham in 1939 (Rex/Shutterstock)

Plate 25 Alan Turing running on 26 December 1946 (Courtesy of King's College Library, Cambridge)



No 83

Copy of letter to a child of ~~seven~~ six, postmark May 10. 53, sent express.

....

Hollymeade
Adlington Road
Wilmslow.

Dear Maria,*

I hope you may get this before you leave tomorrow, as it will give you something to do in the train. It is just to tell you how to do the solitaire puzzle. In the list of moves the numbers show the place to be taken and "____" means it is to be taken by a move horizontally , and " | " that it is vertical.The moves are

		1	2	3		
		4	5	6		
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
		28	29	30		
		31	32	33		

18—, 25 | , 18 | , 10— , 20 | , 11— , 12—, 11 | , 25 | , 30 |, 9—, 4 |, 2—, 9 |, 4 |, 9— , 8 — , 29— , 25 |, 24—, 32—, 25 | , 30 | , 25 —, 15 —,16 —, 22—, 23—, 15 |, 9— , 10 | .

I find it helps if I am trying to do the puzzle to use 4 kinds of pieces like this or better still use a board with the squares in 4 colours. Each piece always stays on the same colour until it is taken . You start with only 4 X's and you must still have one at the end and so you must be very careful of them. But there are 12 O's to be got rid of. One needs to remember this

		○	△	○		
		•	×	•		
○	△	○	△	○	△	○
•	×	•	×	•	×	•
○	△	○	△	○	△	○
		•	×	•		
		○	△	○		

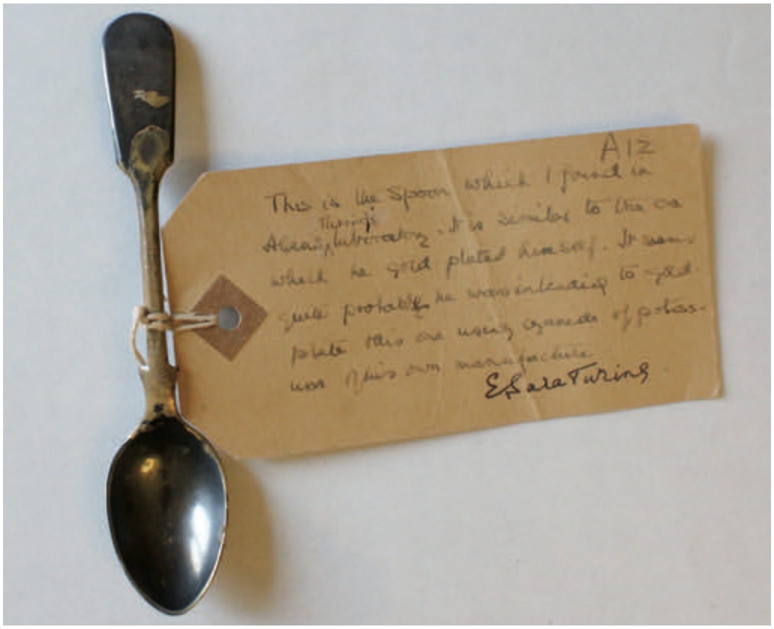
all the time.

I hope you all have a very nice holiday in Italian Switzerland . I shall not be very far away at Club Méditerrané,
Ipsos-Corfu, Greece.

Yours
Alan Turing.

*Maria, a little girl of 6, of whom Alan was very fond
She reciprocated his affection: she kept this letter long after Alan's death
More than ten years later she wrote of her very clear remembrance of him

Plate 26 Transcribed note of Alan Turing on 'how to solve a solitaire' (Courtesy of King's College Library, Cambridge)

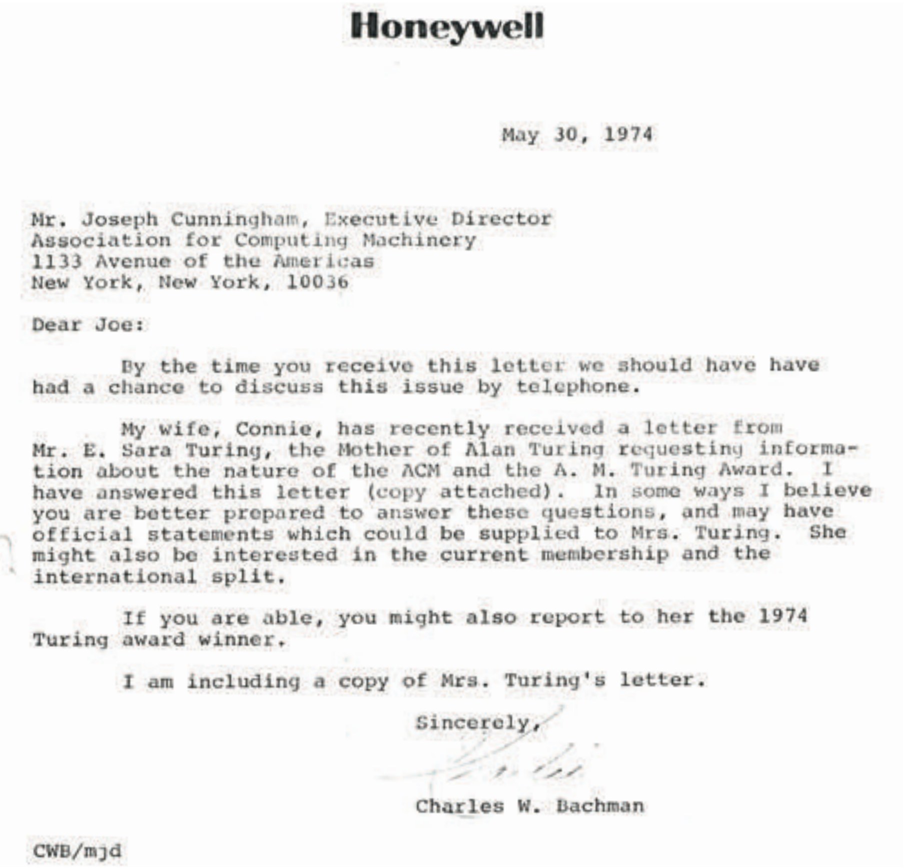


A12

This is the spoon which I found in Alan's Turing's laboratory. It is similar to the one which he gold plated himself. It seems quite probable he was intending to gold plate this one using cyanide of potassium of his own manufacture

E Sara Turing

Plate 27 Teaspoon, with handwritten label by Sara Turing stating, 'This is the spoon which I found in Alan Turing's laboratory' (Courtesy of King's College Library, Cambridge; permission to reproduce Sara's label courtesy of Sir Dermot Turing)



Honeywell

May 30, 1974

Mr. Joseph Cunningham, Executive Director
Association for Computing Machinery
1133 Avenue of the Americas
New York, New York, 10036

Dear Joe:

By the time you receive this letter we should have have had a chance to discuss this issue by telephone.

My wife, Connie, has recently received a letter from Mr. E. Sara Turing, the Mother of Alan Turing requesting information about the nature of the ACM and the A. M. Turing Award. I have answered this letter (copy attached). In some ways I believe you are better prepared to answer these questions, and may have official statements which could be supplied to Mrs. Turing. She might also be interested in the current membership and the international split.

If you are able, you might also report to her the 1974 Turing award winner.

I am including a copy of Mrs. Turing's letter.

Sincerely,

Charles W. Bachman

CWB/mjd

Plate 28 Correspondence regarding the inauguration of the Alan Turing Award (Courtesy of King's College Library, Cambridge)

Plate 29 Quantum Key distribution system (Andrew Shields, Toshiba Research, Cambridge)