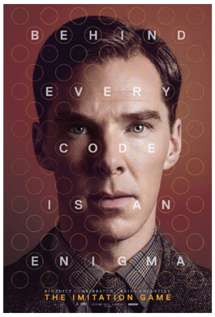
Lost without translation: Why codebreaking is not just a numbers game

NIGEL VINCENT and HELEN WALLACE



The recent film *The Imitation Game* has portrayed the part played by the mathematician Alan Turing in decrypting the messages sent from the German Enigma machine in the Second World War. But Nigel Vincent and Helen Wallace remind us that other skills – particularly in languages – have always been needed in order to understand an enemy's secrets.

Nigel Vincent is Professor Emeritus of General and Romance Linguistics at the University of Manchester, and a former Vice-President for Research and Higher Education Policy at the British Academy. Helen Wallace is Foreign Secretary of the British Academy; both of her parents worked at Bletchley Park in the Fusion Room.

If and when you go to war, the chances are your enemies will speak a different language from that of your own troops. It is also likely that they will seek to disguise their communications by enciphering them, so if you want to eavesdrop on their activities you face a double barrier: you have to crack the code and you have to understand the language. Finally, to turn the intercepted messages into usable military intelligence requires a capacity to link them to the map of where the opposing military units are located and how they might be planning their operations. To achieve this triple task requires a formidable combination of skills: mathematical, engineering, linguistic and analytical. Failure on any one of these fronts will render progress on the other two impossible or worthless.

The back story

There is some evidence of encryption in the ancient world, in Egypt as far back as around 1900 BC, in classical Greece, and to a limited extent in the Roman world (the Romans were hampered by their clunky system of numerals). The term *cipher* derives ultimately from the Arabic word *ṣifr* meaning 'zero, empty', a concept introduced to Europeans by Arab scholars. Interestingly – and how ironically – one of the pioneers of cryptography was Al Kindi (*c.* 801-873 AD), an Iraqi Arab born and educated in Basra. He was the archetypal polymath, a talented mathematician, a philosopher, a theoretician of music – the list of accomplishments goes on. In particular, he introduced the notion of frequency analysis as a tool for cracking codes (Figure 1).

Over subsequent centuries Arab, and later European, intellectuals – not least those who worked for the Roman Catholic Church – developed cryptography and cryptanalysis for military purposes but also for messages that demanded political or commercial confidentiality. However, big scientific breakthroughs in the field did not come until the 19th century. Amongst others Charles Babbage, elected a Fellow of the Royal Society (FRS) in

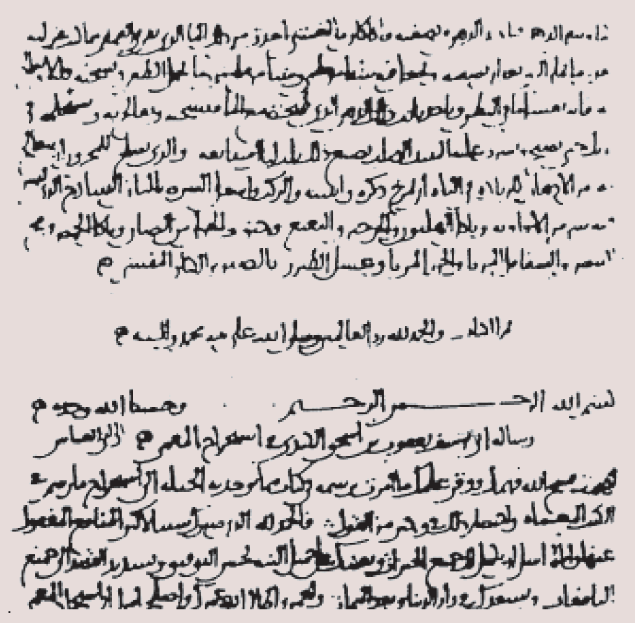


Figure 1
The first page of Al Kindi's manuscript 'On Deciphering Cryptographic Messages', containing the oldest known description of cryptanalysis by frequency analysis. Image: Wikimedia Commons.

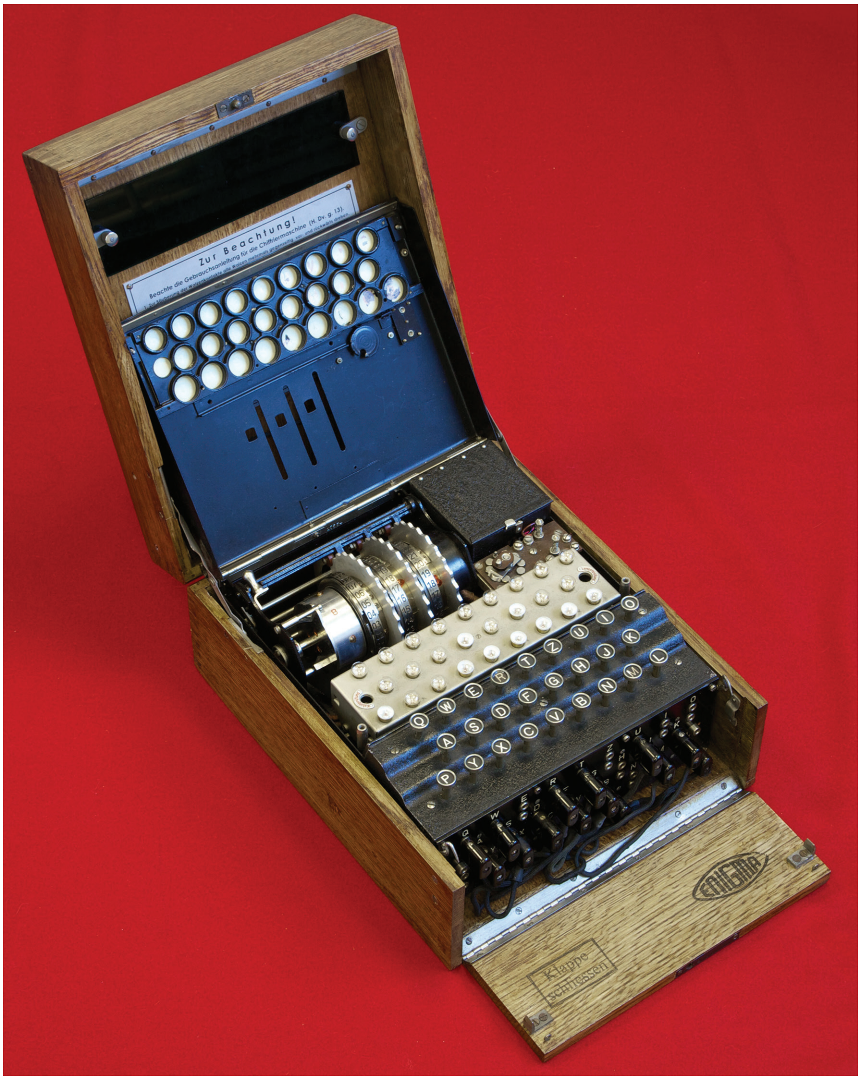


Figure 2
The Enigma machine. © ShaunArmstrong/mubsta.com

1816 at the tender age of 25, was to produce a seminal work on polyalphabetic ciphers. This was written during the Crimean War after he had cracked the Vigenère autokey cipher in use by the Russian army, but publication was withheld on the grounds of military secrecy, his intellectual property rights not being established until 1985 (sic).

Into the modern era

It was in the period of the First World War that cryptography and cryptanalysis started to take off as systematic tools of military intelligence. Mathematicians and engineers in France, Germany, the US and the UK began to develop sophisticated techniques for encrypting their military communications with varying degrees of success in achieving impregnability.

In Britain, with the outbreak of war the naval intelligence team based in Room 40 of the Admiralty took the lead in building capacity for cryptography (the army had a separate unit) and was managed by Sir Alfred Ewing FRS FRSE, an engineer.[1] Other recruits included mathematicians, linguists and classicists, several of whom were academics and who went back to distinguished academic careers after the war. These included: Frank Adcock FBA, classicist; John Beazley FBA, classical archaeologist; Francis Birch, historian; Dilly Knox, papyrologist. The link with Classics here is no coincidence. At the time it was considered a particularly appropriate degree for the very bright, even to the point that as late as 1955 the future Nobel Prize winning physicist, Anthony Leggett, entered Oxford on a Classics scholarship.[2] Classics too had links to the great 19th-century traditions of the decipherment of Egyptian hieroglyphics and cuneiform Hittite and other ancient middle eastern languages. In addition, classical scholars were used to dealing with partial texts and fragmentary evidence, skills that were to prove invaluable when breaking and interpreting coded messages.

During the inter-war years the UK developed its Government Code and Cypher School, which subsequently moved to Bletchley Park, and gradually strengthened its core team of mathematicians, engineers, classicists and other linguists and humanities scholars. Work there was famously associated with breaking messages sent from the Enigma machine (Figure 2), which had been invented as a piece of private enterprise by Alfred Scherbius, a German engineer, who patented it as a commercial device in 1918/19. The German Navy and later the German Army adopted modified versions in the 1920s. When William Friedman, who first decrypted the corresponding, though differently constructed, Japanese Purple machine, headed the American Signals Intelligence Service in the same period, he deliberately set out to recruit staff who were qualified both as mathematicians and as linguists.[3] The case of Japanese Purple also serves to illustrate the fact that it is not sufficient to break a cipher; the results also have to be properly deployed. Whether there was a deliberate attempt to conceal what they knew, or whether there was simply what has been called a 'failure of imagination' on their part, the fact remains that codebreaking had helped to make the US government aware of Japan's hostile intentions already before the attack on Pearl Harbor.

[1] Patrick Beesly, *Room 40. British Naval Intelligence 1914-18* (Hamish Hamilton, 1982), chapter 2.
[2] www.nobelprize.org/nobel_prizes/physics/laureates/2003/leggett-bio.html
[3] R.W. Clark, *The Man who Broke Purple* (Little Brown & Co, 1977).

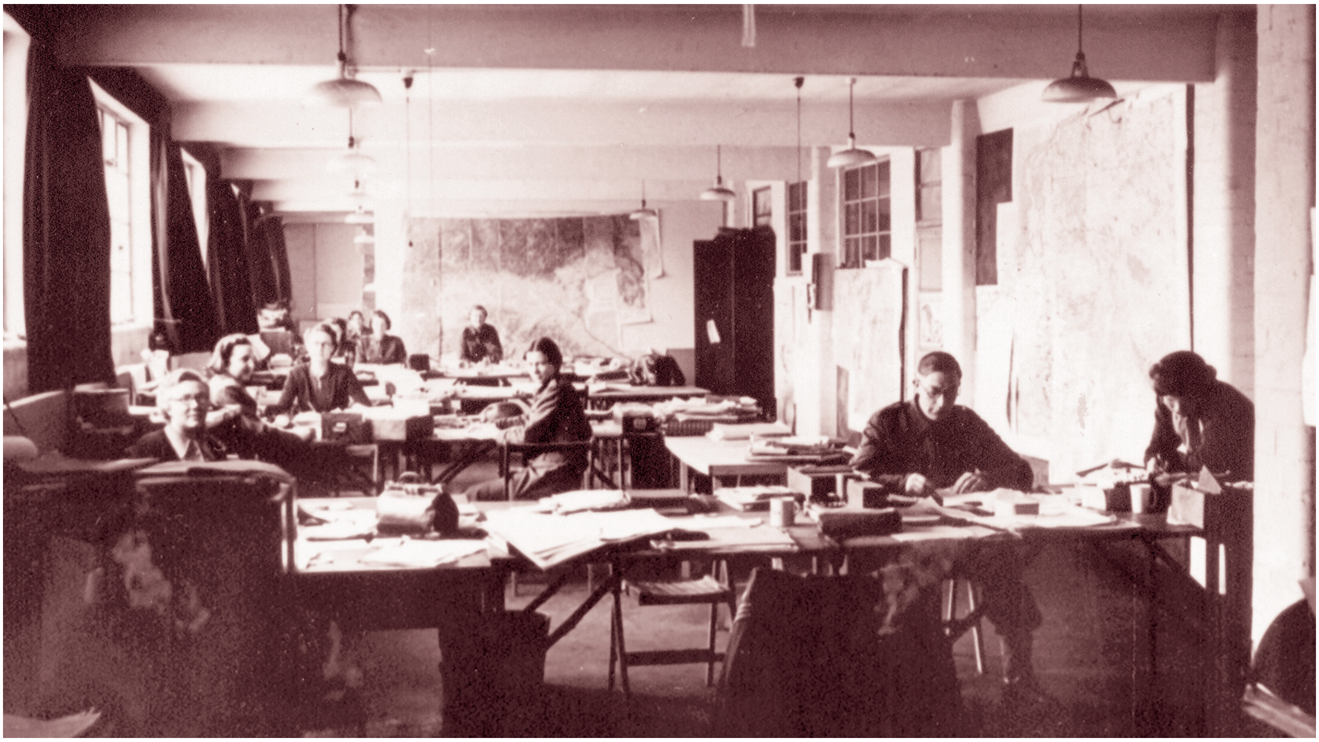


Figure 3
The SIXTA traffic analysis group in the Fusion Room at Bletchley Park during the Second World War. The Fusion Room was where decrypted German army and air force messages were compared with the corresponding data extracted by the log readers from radio traffic between enemy stations so as to build up a wireless telegraphy picture of those units, which was in turn interpreted geographically to identify patterns and positions of German military operations. As the war went on, this task of collation and interpretation became more important, and the Fusion Room became the core of SIXTA. This drew together the intelligence work of Hut 3 with the cryptographic work of Hut 6.

In the centre of the photograph is Joan Thirsk (née Watkins, 1922-2013), who would become a leading economic and social historian and was elected a Fellow of the British Academy in 1974. Helen Wallace's mother, Joyce Robinson, may also be in this picture; her father, Edward Rushworth, was responsible for liaison between the Fusion Room and Hut 3.

© Crown Copyright, reproduced by kind permission of Director GCHQ.

Bletchley Park

The story of Bletchley Park (BP), the centre of the British code-breaking operation during the Second World War, stayed a well-hidden secret until the 1970s, but is now widely recounted and sometimes dramatised as in the film *The Imitation Game*, which focuses on Alan Turing FRS, the very talented mathematician. In the film, as in the simple version of the story, it was the mathematicians who lay at the heart of the success of the British, with early help from clever Polish cryptographers and later contributions from American colleagues. The challenge of the sophisticated Enigma machine and subsequently the Lorenz machine (dubbed Fish or Tunny), the enhancement of statistical methods, and the building of proto-computers of course meant that skilled mathematicians were essential – as indeed were the engineers, among whom Tommy Flowers, who built the Colossus machine to facilitate decrypting. But, however great their success, the fruits of their labours had to be turned into words, and the words turned into usable meaning. Just as in the First World War, so in the Second, Bletchley Park needed other kinds of skills and talents to complement those of the cryptanalysts and the engineers.

So the leadership of BP – and the other cognate military units dealing with signals intelligence and decryption – set about a huge recruitment drive to find more of these other kinds of people. Yes, of course some of these were already fluent in German and to an extent Italian, Japanese or Russian, and many were people whom we would now call lateral thinkers. The recruiters trawled the universities – mostly but not only Oxbridge – for talented academics and promising students. They were able to find an impressive range of men and women, most of whom quietly reverted to their former lives after the end of the war. Many of these went on to impressive academic careers in their specialist fields, Among these some 29 were in due course to be elected Fellows of the British Academy (FBA),[4] including J.L. Austin, Carmen Blacker, Asa Briggs, John Chadwick, F. Harry Hinsley, Peter Laslett and Joan Thirsk (Figure 3).

Why were these people so important? First, as we can all understand from using our mobile phones and texting, poor signal can fracture a call and idiosyncratic

[4] An initial trawl from both written and oral sources has yielded the names of some 73 humanities scholars who worked at BP and cognate units and went on to academic careers, among whom the 29 Fellows of the British Academy. In this 70th anniversary of the end of the Second World War, the British Academy is seeking to commemorate, by means of a simple list, those men and women who helped bring about victory through their work in military intelligence and who were already or would go on to become humanities academics. The initial list has been posted on the British Academy's website, and we would welcome information on names that should be appropriately added – see www.britishacademy.ac.uk/ww2intelligence

shorthand has to be interpreted, so just getting the message itself into readable language was not straightforward. Secondly, the source and destination of the message had to be identified from recognition of the intercepted call signals and then plotted on the map of military units. Thirdly, the content of the message had to be functionally interpreted – it seems that those classicists who understood the Roman army were particularly skilled at this! A very great deal could be lost in translation. Fourthly, many of the messages were not decrypted in real time, and hence the sequencing of the messages had to be carefully plotted and analysed. Thus it was, for example, that several days after a message from a German unit during the liberation of Yugoslavia had been read in the Fusion Room at BP, it was realised that a stray Red Army unit was on its way to Tito's hideout and SOE was able to beat them to it.

What lessons can we draw from this? The successes of BP were due to the combination of talents, skills and ingenuities of men and women with a wide array of backgrounds; this was functioning interdisciplinarity at its best. It drew on what nowadays we call the STEM subjects, but it needed the insights from the humanities – linguists and others (there were not so many social scientists in those days). It presupposed that there was a pool of bright people in the academic community who could deploy what we might now badge as transferable skills that most of them had probably never dreamed they had.

It is interesting to reflect too on the relation between the language needs at the time and the provision that was available through the British educational system. In an age when most if not all pupils in grammar schools studied at least French and usually German, there was a ready supply of qualified people coming through into degree level work. Russian too was important and, although less widely studied at secondary level, there were a number of university departments up and down the country that could provide the relevant expertise and tuition. As the global conflict extended, so more languages came into the picture. The Director of the School of Oriental and African Studies (SOAS) had already warned the War Office in 1939 that there would be a need for other language skills, but it took until 1942 for the War Office to introduce its own intensive 6-month Japanese course from a base in Bedford. The Department of Linguistics and Phonetics at SOAS subsequently devoted its energies to running courses in Japanese and also Chinese, Farsi and Turkish for prospective service personnel. In teaching these new and understandably demanding students, staff did, however, have the advantage that, as we have said, by and large the people in their classes would have already studied one or more modern language and probably some Latin and Ancient Greek at school. It is always easier to teach a new language to someone who already has a couple under their belt.

When it came to more particular needs, say the languages of the Balkans or south-east Asia, there were small but specialist departments with qualified personnel on hand. SOAS for example was founded in 1916, and London's School of East European and Slavonic Studies

J.L. [John Langshaw] Austin (1911-1960), a philosopher at the University of Oxford, was one of many humanities scholars who brought their varied skills to bear on interpreting enemy intelligence in the Second World War. He was elected a Fellow of the British Academy in 1958. The following is an extract from his Obituary Notice in Proceedings of the British Academy*, 49 (1963).*

After a spell of preliminary training at Aldershot and Matlock in the summer of 1940, he had been commissioned in the Intelligence Corps and posted to the War Office in London. His first important employment was on the German Order of Battle, work which demanded exactly the kind of detailed accuracy which was, of course, immensely congenial to him. But in 1942 he took over the direction, at G.H.Q. Home Forces, of a small section which had recently been formed, to do the preliminary intelligence work for an invasion of Western Europe; and this was the field in which he became an unrivalled authority. His section, whose earlier days had been rather haphazard, was soon operating with method, rapidity, and a clear purpose. Though his standards were exacting, those under his command were enlivened by the confident sense of solid work getting done, of real progress being made. Professor A.J. Beattie [Professor of Greek, University of Edinburgh], who served with Austin at this time, records that 'his superiors in rank very quickly learned that he was an outstanding authority on all branches of intelligence work, and they soon depended on his advice far more than would normally have been considered proper in any headquarters'.

In the following year Austin's section was vastly enlarged and transferred, under the name of the Theatre Intelligence Section, to 21st Army Group. Of this larger affair Austin as a Major – and later, when S.H.A.E.F. was formed, a Lt.-Col. – was of course not formally in command; but by this time his knowledge was so voluminous, his expertise so great, and his judgement so highly valued, that in practice he continued in charge of all the work. Before D-Day he had accumulated a vast quantity of information on the coast defences of northern France, on the base areas, supplies, formations, and transport system behind them, and indeed on every aspect of the German defence forces and civilian administration in that 'theatre'. Weekly, and later daily, reports were issued recording changes in the German dispositions; and a kind of guidebook was compiled for the use of the invading troops, in whose title – *Invade Mecum* – those who know Austin's writings will recognize his style. It has been said of him that he directed this huge volume of work 'without ever getting into serious difficulty of any kind' and, more impressively, that 'he more than anybody was responsible for the life-saving accuracy of the D-Day Intelligence'.

had come into existence a year earlier. They could not of course contain experts in every one of the world's 6000 or so languages, but their broad knowledge of the language families and their geographical and cultural distribution meant they were well placed to offer advice and guidance in the event of urgent need. It must be a matter of national concern that many such centres have been closed or the range of languages covered has been reduced in the years between then and now.

The contemporary world

Nowadays the cryptography side has been pretty well totally taken over by computational methods and the advent of the cyber world. Arguably, too, even the basics of translation can be handled by algorithms of the kind that underlie Google Translate, which are based not on traditional modes of grammatical and structural analysis but on statistical patterns of recurrence over the very large bodies of texts that make up the daily activity of the internet. Hence, different kinds of skills and different forms of interdisciplinarity are now required. For the most part contemporary wars and conflicts are conducted within countries rather than in the classic forms of inter-state confrontation. This state of affairs exacerbates the need for mastery not only of formal written language but also of the informal and colloquial dimensions of language which are well beyond what computational methods can handle. Moreover, such skills need to be accompanied by deep historical and cultural understanding if we are to get to grips with the complex societal fissures that prompt conflicts, condition modes of action and hamper peacekeeping. A recurrent theme in books such as Mike Martin's *An Intimate War: An Oral History of the Helmand Conflict 1978-2012* and the essays by military leaders collected in *British Generals in Blair's Wars* is the way lack of knowledge of local languages and cultures led to our troops being misled or worse.

The picture is further complicated by the fact that the needs of the contemporary world are for languages that are off the European and Oriental beaten tracks – for example Hausa in West Africa; Somali to deal with modern piracy; Pashto in the Afghanistan conflict – and in countries where multilingualism is the norm. There are for example 13 recognised national languages in Mali and some 60 indigenous languages in South Sudan, where paradoxically the only official language is English. It is in this context that the review of the national need for languages contained in the British Academy's report *Lost for Words* (2013) was conceived. We can do no better than quote the leading recommendation of that report: 'There needs to be a cross-government strategy for language capacity that identifies the language capabilities and requirements of government, and supports the development of these skills.'[5]

Conclusion

Unfortunately, the world is a troubled place and the need for this array of talents does not diminish. It is to be welcomed that the British Army has a culture and foreign language strategy, that the Ministry of Defence has recently enhanced its Defence Centre for Languages and Culture, and that the Foreign and Commonwealth Office has reopened its Foreign Language School. However, these have to be underpinned by an urgent effort across the educational sector to instil language competences as normal and useful, to maintain centres of specialised expertise on other countries and regions, and to promote the need for combining efforts through habits of functional interdisciplinarity. So, as we reflect on the past successes at BP, we must celebrate the achievements of those who contributed across this range, and learn from their example.

[5] *Lost for Words: The Need for Languages in UK Diplomacy and Security* (British Academy, November 2013), p. 13. For more on the British Academy's programme to target deficits in languages, see Nigel Vincent, 'Why English isn't enough: Debating language education and policy', *British Academy Review*, 24 (Summer 2014), 10-12. Also go to www.britishacademy.ac.uk/languages