March 2005
Features

Exploring the Enigma

by Claire Ellis

As long ago as the Ancient Greeks, warring armies have encrypted their communications in an attempt to keep their battle plans a secret from their enemies. However, just as one side invented an ingenious new way to encipher its messages, so would its enemies discover a clever way of cracking that code. The result has been that codes and ciphers have become more and more complex and increasingly difficult to crack over time, as, throughout history, an intellectual battle has raged between code makers and code breakers.

The battle of wits was never keener than during the Second World War, when the Germans used the famous Enigma machine − which they believed uncrackable − to encode messages, and the Allies worked at Bletchley Park to decipher the code.

The birth of an enigma

German soldiers using an Enigma machine during the second world war

Up till the Second World War, the most advanced forms of encryption involved simple paper and pencil techniques. But security blunders on both sides during the First World War highlighted a need for a higher level of secrecy, with more advanced methods of enciphering messages. Both the Allies and the Axis countries were looking for a new way to encrypt messages − a way that would result in complete security. (For more information, have a look at our explanation of the basic terminology of codes and ciphers.)

In 1915 two Dutch Naval officers had invented a machine to encrypt messages. This encryption tool became one of the most notorious of all time: the Enigma cipher machine. Arthur Scherbius, a German businessman, patented the Enigma in 1918 and began selling it commercially to banks and businesses.

The Enigma machine's place in history was secured in 1924 when the German armed forces began using a specially adapted military version to encrypt their communications. They continued to rely on the machine throughout the Second World War, believing it to be absolutely unbreakable.

How the Enigma machine worked

A diagrammatic representation of an Enigma machine

When a plaintext letter was typed on the keyboard, an electric current would pass through the different scrambling elements of the machine and light up a ciphertext letter on the "lamp board". What made the Enigma machine so special was the fact that every time a letter was pressed, the movable parts of the machine would change position so that the next time the same letter was pressed, it would most likely be enciphered as something different. This meant that it wasn't possible to use traditional methods to try and crack the notorious cipher.

To make things even more difficult, different parts of the machine could be set up in different ways, with each setting producing a unique stream of enciphered letters. Unless you knew the exact settings of the machine, you couldn't decipher the messages.

How many ways are there to set up an Enigma Machine?

Choosing Rotors

An Enigma machine rotor. Copyright Simon Singh

Army issue Enigma machines had three revolving "wheels" or "rotors" that could be taken out and changed about.The first task for an Enigma operator would be to decide which rotor went in which position. There were five rotors to choose from and they could be inserted into three positions on the Enigma machine.

- **Question 1**: How many possible ways are there of positioning 5 rotors in 3 slots in the Enigma? (Check your answer.)

The rotor starting positions

- **Question 2**: Once you have chosen the order of the rotors, how many possible ways can you set the starting positions of the rotors?
(Check your answer.)

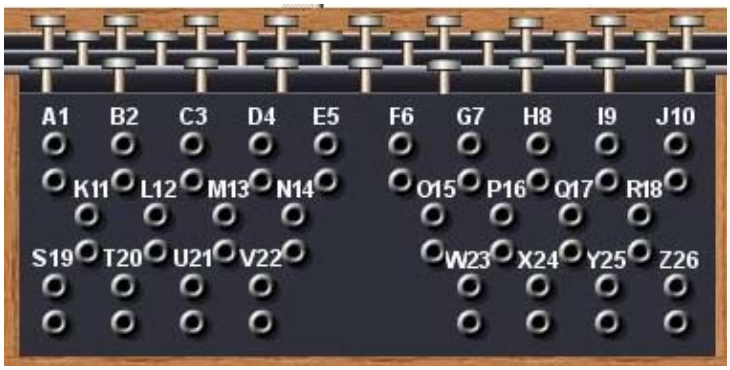
The ring settings

Every time a letter was pressed on the keyboard, the rotor on the far right would move around one place. Once it had completed a full revolution (ie moved forward 26 places), it would kick the middle rotor forward one position. When it had completed another revolution, it would again kick the middle rotor forward one position. When the middle rotor had completed a full revolution, it would kick the left−hand rotor forward.

The point at which the right hand rotor kicked the middle rotor forward and the point at which the middle rotor kicked the left hand rotor forward could be changed. This was called the "Ring Setting".

- **Question 3**: How many possible "Ring settings" were there on a 3−rotor army Enigma?
(Check your answer.)

The plugboard



A diagrammatic representation of the plugboard

On the front of the machine was another section called the "plugboard". The Enigma machine had several cables with a plug at each end that could be used to plug pairs of letters together. If A were plugged to B then, on typing the letter A, the electric current would follow the path that was normally associated with the letter B, and vice versa.

Enigma machines had 10 cables with which to link up pairs of letters.

- **Question 4**: How many ways are there to link up pairs of letters on the Enigma machine?

The answer is that there are approximately 150,000,000,000,000 − that is, 150 million million − possible combinations of 10 pairs of 26 letters on the plug board. The maths behind this calculation is complex, but a full explanation is given at http://www.codesandciphers.co.uk/enigma/steckercount.htm, a page from Tony Sale's website.

Therefore, the total number of possible ways in which a standard army−issue Enigma machine could be set up was:

$$60 \times 17,576 \times 676 \times 150,738,274,937,250,$$

which is approximately 158 million million million.

Deciphering Enigma

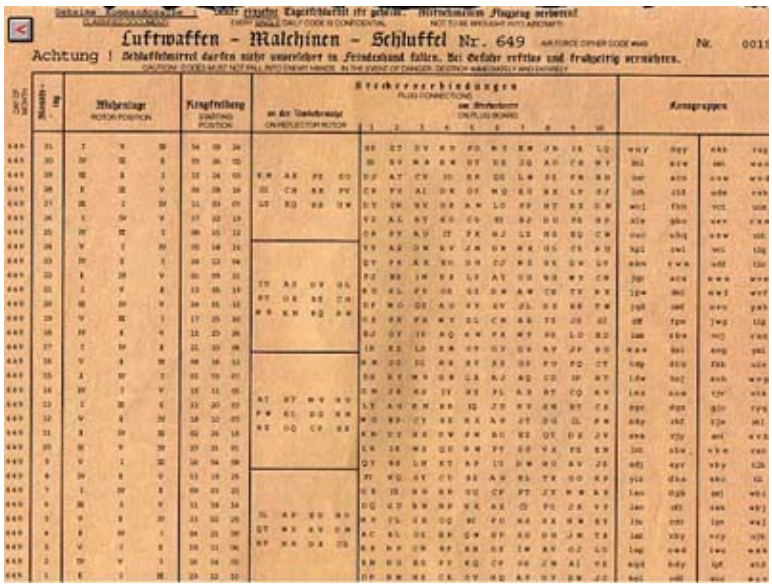
When the Enigma machine is used, the Enigma machine itself is the algorithm; the way in which it is set up is the key. Just as with any other type of cipher, as long as the recipient knows the key, the process of deciphering an Enigma encrypted message is incredibly simple. A German soldier receiving an enciphered message simply had to type the ciphertext letters into his own Enigma machine. If his machine was set up exactly in exactly the same way as the message sender's, then the plaintext letters would appear on the lamp board.

However, just as with any other type of cipher system, if you don't know the key it is very difficult to read the message − even if you know which system was used to encipher it.

The British had set up listening stations (called *Y Stations*) all over Britain, so that they could eavesdrop on the German military. Even though the Allies had managed to get hold of Enigma machines, in order to decrypt the messages they intercepted they needed to know the key To make it as difficult as possible for the Allies to decipher messages, the Germans would change the key every day, resetting their Enigma machines at

midnight every night.

Agreeing on a key


Luftwaffen - Maschinen - Schlüssel Nr. 649

A monthly keysheet

Cipher machine operators were issued with a Key Sheet every month, which told them how to set up their Enigma machines for every day that month. There was an obvious security flaw: if the Allies recovered a key sheet, they would be able to read the Enigma messages.

For this reason, Key Sheets were extremely closely guarded and were printed in soluble ink. If it ever looked as though a Key Sheet might be captured by the Allies, German soldiers would dip it in water and wash off all the information.

The Germans believed the strength of the Enigma lay in the fact that it was impossible to work out the key from the billions and billions of potential keys every single day. As long as the Allies did not get hold of the key sheet, their communications would remain secure.

The work at Bletchley Park

Bletchley Park. Copyright Bletchley Park Trust

In August 1939 the British established the Government Code and Cipher School at Bletchley Park in Buckinghamshire. The people recruited to work there came from a variety of backgrounds. There were experienced codebreakers, secret service officers, mathematicians, scientists, crossword experts, international chess players, students, actresses and even astrologers and debutants.

Fortunately for the British codebreakers, in the years running up to the war Poland had worked on various techniques for cracking Enigma. Shortly before the German invasion of Poland, they shared their work with their British allies. Poland's government was the first to employ mathematicians as code−breakers, and the mathematicians' logical minds proved to be just what was needed to tackle Enigma.

This vital headstart from the Polish, coupled with the unique problem−solving and intuitive thinking skills of Bletchley's recruits, meant that Enigma was cracked in early 1940 a reliable technique for cracking Enigma was established. The British code breakers worked in shifts around the clock for the whole of the war, using paper and pencil as well as newly invented mechanical techniques to work out the particular Enigma machine settings for each and every single day.

Unwittingly, the Germans themselves helped the British to decipher the Enigma. For example:

- Messages often began with the same opening text − many began with the word *Spruchnummer* (Message Number), and many Air Force messages began with the phrase *An die Gruppe* (To the Group).
- Messages often enciphered routine information such as weather reports and phrases such as *Keinebesondere Ereignisse* (Nothing to report).
- Messages often ended with *Heil Hitler*!
- The Germans often transmitted the same message more than once, with each version enciphered differently.

These lapses provided the codebreakers with clues, called *cribs*, about how the Enigma machines had been set up on that day. These cribs were essential for breaking the ciphers. For example, without a crib it would still take several months today to decipher an A4 page of ciphertext using a modern PC with trial and error methods.

However, the cribs alone were not enough. The codebreakers at Bletchley Park developed new procedures and algorithms for determining the set−up of the Enigma and also had to develop electronic computing devices to implement these methods.

Today, historians believe that the work of the code breakers at Bletchley Park shortened the war by two years.

Neglected heroes

Among the most famous of the leading code breakers at Bletchley Park was a mathematician from the University of Cambridge, Alan Turing. Turing was regarded by many as a genius. He played a leading role in breaking the more complicated Naval Enigma cipher (codenamed Shark) and also established the principles behind the modern computer.

Despite their remarkable work, however, for a long time afterwards none of the second world war code breakers received the public recognition they deserved. In order to preserve British security, the breaking of Enigma remained a tightly guarded secret for the duration of the war, and for the following 30 years. The people who had worked at Bletchley Park were forbidden from talking about what they had done and as a result their contribution to the war effort was entirely forgotten. However, over the past 30 years more and

more information has been released about the incredible story of Bletchley Park.

Tragically, for some, however, the acknowledgments have come too late. Alan Turing committed suicide before he was ever publicly recognised for his extraordinary part in the war and before his contributions to the science of codes and code breaking were fully understood.

The British Government still operates a code breaking department, at "Government Communication Headquarters" in Cheltenham. And to this day they rely on mathematicians for their problem solving abilities and logical thinking: GCHQ boasts the highest concentration of pure mathematicians in the country. Today's secret codes are much more sophisticated than the Enigma cipher and their strength relies on the inability to factorise large numbers, so with today's worries about global terrorism, the role of our code breakers is just as vital as during the second world war.

More information

- The Enigma Project:
  The MMP's outreach project which takes codes, code breaking and a genuine WW2 Enigma machine into the classroom.
- Bletchley Park:
  Find out about WW2's code breaking heroes and information on breaking Enigma. Bletchley Park is now a museum and information about visiting can also be found on their website.
- NRICH Maths:
  The March 2004 issue (select this on the left hand menu) is all about different secret codes with puzzles to break.
- National Cryptologic Museum:
  The US National Security Agency's museum of cryptography.
- Simon Singh's Crypto Corner:
  Information about a host of different codes. The story of the Code Book Cipher Challenge, who won it and how. Also links to other cryptography websites. Follow links to the Black Chamber for on−line puzzles and decryption tools. You can also download free copies of the Code Book CD−ROM.
- Alan Turing Memorial:
  Information about Alan Turing's memorial statue in Manchester.
- Codes and Ciphers:
  All you ever wanted to know about Second World War codes and ciphers.

Answers to the questions in the text

Answer 1

For the first slot, you can choose any one of 5 rotors. For the second, you can choose any one of 4 rotors. For the last, you can choose any one of 3 rotors. So there are

$$5 \times 4 \times 3 = 60$$

ways of positioning 5 rotors in 3 slots.
Back to question 1.

Answer 2

As there are 26 letters of the alphabet, each of the 3 rotors could be set in any one of 26 different starting positions. This gives a total of

$$26 \times 26 \times 26 = 17,576$$

distinct starting positions.
Back to question 2.

Answer 3

The first ring can be set in any of 26 positions, as can the second, so there are

$$26 \times 26 = 676$$

ways of positioning the 2 rings on a 3−rotor army Enigma.
Back to question 3.

About the author

Claire Ellis has recently joined the Millennium Mathematics Project, the Cambridge−based mathematics enrichment and dissemination group that publishes *Plus* magazine. She runs the Enigma Project.

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.