20 Enigma Cipher

Introduction

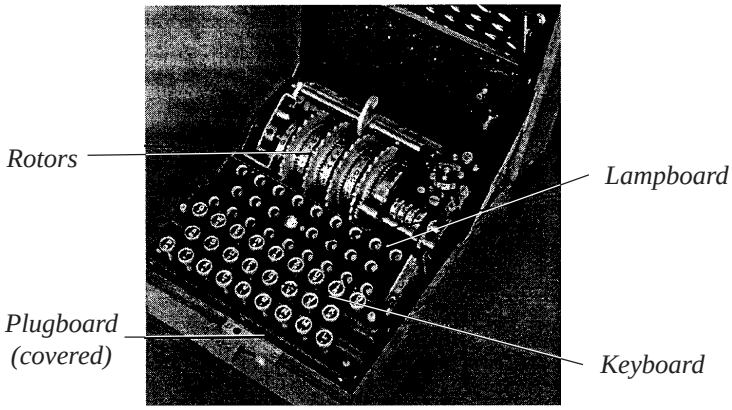
Security blunders on both sides during the First World War increased the need for a higher level of secrecy and more advanced methods of enciphering messages other than traditional pencil and paper techniques.

In 1915, two Dutch Naval officers 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 1926 when the German armed forces began using a specially adapted military version to encrypt their communications. They continued to rely on the machine throughout World War II, believing it to be absolutely unbreakable.

How the Enigma machine worked

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 'lampboard'. What made the Enigma machine so special was the fact that every time a letter was pressed, the moveable 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 traditional frequency analysis methods could not be used to crack the code.



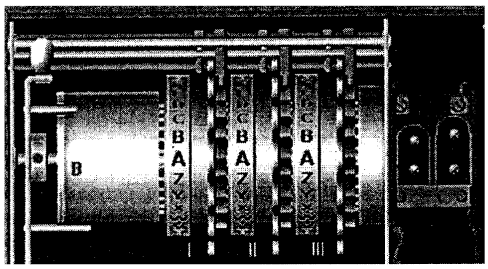
World War II Enigma Cipher Machine

To make it 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 setting of the machine, you couldn't decipher the messages.

Choosing rotors

Inside the Army issue Enigma machine there were 3 cipher wheels called *rotors* which could be taken out and changed about. Each rotor had the letters A to Z with different

internal wiring systems. There were 5 rotors that the Enigma operator could choose from for the 3 slots in the machine.



Rotors in position in an Enigma Cipher Machine

Diagram of an individual rotor

Exercise 1

How many ways are there of positioning the 5 rotors in the 3 slots in an Enigma machine?

Starting position of rotors

The rotor starting point could be any one of 26 different positions (one for each letter of the alphabet).

Exercise 2

In how many different ways can you set the starting position of the rotors?

Ring settings

Each time a letter was pressed on the keyboard, the rotor on the far right would move around one place. At one particular position it would kick the middle rotor forward one position. Then after a further complete revolution it would again kick the middle rotor forward by one position. Likewise the middle rotor at one of its positions would kick the left hand rotor forward by one position. The system was similar (but not identical to) a milometer in a car except that a revolution would involve 26 steps forward rather than 10. (In fact the movements of the middle rotor were slightly more complex than has been described here.)

Each rotor had a metal ring attached to its circumference marked with the letters A–Z. The rings could be moved round the inner cores of their rotors and then locked at chosen positions. These three chosen positions were known as the **ring settings**. The chosen settings did not affect the basic electrical configuration of the machine, but one thing they did was to fix the positions at which the forward movements of the middle and left rotor occurred.

We are now in a position to determine the number of possible ways of setting up the rotors. It will be

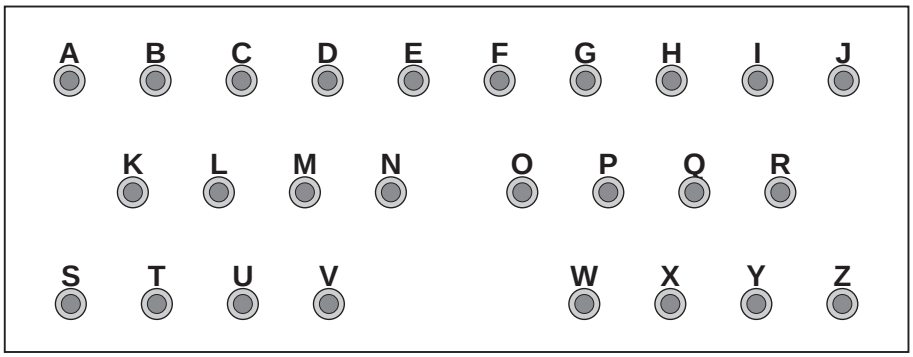
$$60 \times 17576$$

No. of ways of positioning 5 rotors in 3 positions × *No. of different starting positions for rotors*

This gives 1 054 560. So already there are already over one million possible settings for the start up position of the machine – but it is even more complicated!

Plugboard

On the front of the machine was another variable section called the *plugboard.* This was used to further scramble the messages, and increase the possible number of ways the machine could be set up.



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

Example

If there was just *one* cable, in how many different ways could the plugboard be set up?

Solution

You could connect A with 25 other letters
B with 24 other letters
C with 23 other letters, etc.

giving

$$25 + 24 + 23 + ... + 2 + 1$$

ways.

You can easily see this as

$$S_{25} = 25 + 24 + ... + 2 + 1$$

$$S_{25} = 1 + 2 + ... + 24 + 25$$

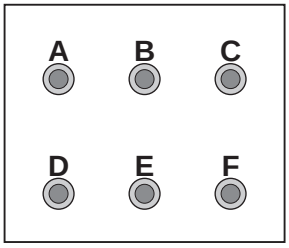
$$2S_{25} = \underbrace{26 + 26 + ... + 26 + 26}_{25 \text{ times}} = 25 \times 26$$

$$S_{25} = \frac{25 \times 26}{2} \qquad \left(\text{or } S_n = \frac{n(n+1)}{2} \right)$$

$$= 325 \text{ ways}$$

To find out the number of connections to use that gives the maximum number of possibilities requires results from combinatories. We will start by working through the following Activity.

Activity 1



With this simplified plugboard, determine how many ways there are of making connections with

a) 1 b) 2 c) 3 cables

What is the optimum number to use?

Activity 1 shows how complicated it can get even with just 6 letters. In fact, the key formula for the number of ways of choosing m pairs out of n objects (n must be an even number) is

$$\frac{n!}{(n-2m)!m!2^m}$$

(A proof is given in Appendix 1.)

Example

In how many ways can you choose 2 pairs from 6 objects?

Solution

Here $n = 6,\ m = 2$, so

$$\text{number of ways} = \frac{6!}{2!\,2!\,2!} = 45$$

(and this is what you should have obtained in Activity 1).

Exercise 3

Check the other two values found in Activity 1.

In fact, with 26 letters the Germans used 10 cables, i.e. 10 pairs.

Example

How many ways are there of choosing 10 pairs from 26 letters?

Solution

$n = 26,\ m = 10$, so from the formula

$$\text{number of ways} = \frac{26!}{6!\,10!\,2^{10}}$$

$$= 150\,738\,274\,937\,250$$

$$\approx 1.5 \times 10^{14}$$

Activity 2

Write a program or use a spreadsheet to evaluate the formula

$$\frac{n!}{(n-2m)!\, m!\, 2^m}$$

for $n = 26$ and $m = 1, 2, ..., 13$

Does the result surprise you?

Finally we can work out the approximate number of ways of setting up the electrical circuits on the three rotor Enigma machine; it is

$$60 \times 17576 \times 1.5 \times 10^{14} = 1.58 \times 10^{20}$$

No. of set-up positions for rotors ↙ ↘ *No. of ways of setting up plugboard*

which is a very large number!

Deciphering Enigma

The process of deciphering was incredibly simple, provided the recipient of the message knew how the Enigma machine had been set up when the message had been enciphered. A German soldier receiving an enciphered message would simply have to type the ciphertext letters into their own Enigma machine. If their machine was set up exactly in exactly the same way as the message sender's, the plaintext letters would appear on the lampboard.

In this way, the *algorithm, or* method of encryption, is the Enigma machine. The *key* is knowing how the machine is set up.

This type of encryption is known as *Symmetric Encryption* because the operation of deciphering is inverse to the operation of deciphering. The decoding key is also the same as the encoding key. This means that if the enemy knows your method of encryption (and during World War II, the Allies knew the Germans were using Enigma), then the key *must* be kept secret. If the enemy uncover the key, this immediately implies cracking of the message thus jeopardising security.

In order to make it as difficult as possible for the Allies to work out the Enigma key, the Germans would change the key every day, resetting their Enigma machines at midnight every night.

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 weakness in this system in that if the Allies were able to recover the key sheets, 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 the key sheet might be captured by the Allies, German soldiers would dip the key sheet 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, they thought that their communications would remain secure.

Whilst the methods used at Bletchley Park are too complicated to fully illustrate here, we can gain some insight into the process by using a 'Paper Enigma'. This is given in Appendix 2.

The rotor settings are given in the first three columns; we will call this the 'message setting'.

Note

All spaces between words to be encoded were removed, otherwise they could often provide clues about the messages, and the letters were then put together, as far as possible, into groups of five. After decoding a message the spaces had to be restored by inspection.

Example

Using the messages setting HAC, encipher the message

AN ENIGMA CIPHER

Solution

Starting on line 3 of the paper Enigma, we see that A $\Rightarrow$ Q. For the next letter, N, you use the next rotor position HAD (line 4) which gives N $\Rightarrow$ F. Continuing in this way, and working in groups of five letters, we obtain

QFREV UISPA JWXH

Exercise 4

Using the same initial rotor setting, HAC*, encipher again the cipher message above.*

This illustrates the ease of deciphering if you know the initial setting of the machine!

Activity 3

Encipher a short message (no more than 18 letters) using the initial position HAA for the rotors. Decipher it in the same way.

The basis for one method of breaking the Enigma cipher was based on having a 'crib'. By this we mean making a correct guess for a small part of the message. In the following simple simulation, we will assume that the unknown message settings actually appear on our list in Appendix 2, so that we should be able to find by investigation correct cipher characters. Each possible setting found can then be tested to see if it leads to the correct deciphering of the complete message.

Example

The cipher message is

GYYLC QJG

but you are told that the first letter in the original message is thought to be S.

Use the crib 'G is the cipher letter of S', to decipher the message.

Solution

By inspecting the table, you can find G ↔ S in both line 9 and line 11. We look at each one in turn.

Line 9

G	Y	Y	L	C		Q	J	G
↓	↓	↓	↓	↓		↓	↓	↓
S	A	L	W	Z		H	O	O

This doesn't seem to make much sense!

Line 11

G	Y	Y	L	C		Q	J	G
↓	↓	↓	↓	↓		↓	↓	↓
S	E	N	D	H		E	L	P

and clearly the message is SEND HELP.

Exercise 5

Try to decipher

NWJCQ HDMYL THXFJ

using the crib that Q is thought to represent A in the original message.

Exercise 6

The last two letters in a cipher message are thought to represent the letters N and E. Use this crib to decipher the message

RDTNP GSUYG KWIZQ

We must not be misled by the simplicity of the above example, in which we only have to search through 18 cipher tables. In reality, a complete version of the 'Paper Enigma' would contain 17 576 different cipher tables and would require a piece of paper more than 220 metres long! Even then, it would only be valid for one set of the initial adjustments made to the machine, and the secret instructions used for making these, could provide many millions of different possibilities. Under these circumstances a crib consisting of only one or two letters would be useless, and normally the crib would have needed to contain about 12 or more letters.

Appendix 1

The number of ways of choosing *m* pairs out of *n* objects

THEOREM

The number of ways of choosing *m* pairs out of *n* objects, where *n* is an even number, is

$$\frac{n!}{(n-2m)m!2^m}$$

PROOF

We are actually choosing $2m$ items from the *n* items.

When choosing the 1st item we have *n* options.

When choosing the 2nd item we have $n-1$ options.

...

When choosing the "$2m$"th item we have $(n-2m)+1$ options.

So in total we have

$$n \times (n-1) \times (n-2) \times ... \times (n-2m+1)$$

This can be written as

$$\frac{n!}{(n-2m)!}$$

Unfortunately, some of these combinations of *m* pairs chosen from *n* items are equivalent to each other. We need to know how many are equivalent to any particular combination.

The *m* pairs can be picked in any order, so there are *m* options for the 1st pair, $m-1$ options for the 2nd pair and so on until there is 1 option for the last pair.

This can be written as

$$m \times (m-1) \times ... \times 2 \times 1 \text{ ways.}$$

So there are $m!$ ways of arranging the *m* pairs.

Each pair can be either way round, so the number of arrangements needs to be multiplied by 2 for each of the *m* pairs. This is the same as multiplying by 2^m.

In total then, a set of *m* pairs has $m! \times 2^m$ equivalent arrangements.

We need to divide the number of ways of choosing $2m$ items by this value because for every $m!2^m$ equivalent arrangements we only need to count <u>one</u>.

Our final number of ways of picking *m* pairs from *n* items is therefore:

$$\frac{n!}{(n-2m)!} \div m!2^m$$

i.e. $$\frac{n!}{(n-2m)!m!2^m}$$

Appendix 2

A 'Paper Enigma' Machine

Shows the ciphers obtained for rotor positions "HAA" to "HAR" using a particular set of adjustments of the machine
(After enciphering each letter from your message, move down to the next rotor settings)

Rotor settings				Enigma Ciphers																							
				A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	**H**	**A**	**A**	W	O	F	S	Y	C	L	X	R	Q	P	G	T	V	B	K	J	I	D	M	Z	N	A	H	E	U
2	**H**	**A**	**B**	O	N	S	Y	T	P	Z	Q	M	K	J	X	I	B	A	F	H	V	C	E	W	R	U	L	D	G
3	**H**	**A**	**C**	Q	E	I	F	B	D	M	U	C	R	W	X	G	Y	S	V	A	J	O	Z	H	P	K	L	N	T
4	**H**	**A**	**D**	P	H	V	M	L	N	Y	B	U	Z	X	E	D	F	W	A	S	T	Q	R	I	C	O	K	G	J
5	**H**	**A**	**E**	S	T	F	H	R	C	O	D	X	U	L	K	W	V	G	Z	Y	E	A	B	J	N	M	I	Q	P
6	**H**	**A**	**F**	R	U	H	X	N	J	O	C	T	F	Q	W	Y	E	G	S	K	A	P	I	B	Z	L	D	M	V
7	**H**	**A**	**G**	Q	C	B	Z	O	R	M	P	V	X	T	W	G	S	E	H	A	F	N	K	Y	I	L	J	U	D
8	**H**	**A**	**H**	T	M	K	W	X	N	U	V	P	S	C	R	B	F	Z	I	Y	L	J	A	G	H	D	E	Q	O
9	**H**	**A**	**I**	Y	C	B	E	D	T	S	Q	M	L	U	J	I	Z	X	R	H	P	G	F	K	W	V	O	A	N
10	**H**	**A**	**J**	S	O	P	M	W	R	I	T	G	U	Q	Y	D	X	B	C	K	F	A	H	J	Z	E	N	L	V
11	**H**	**A**	**K**	X	D	P	B	F	E	S	V	R	T	Z	W	Q	U	Y	C	M	I	G	J	N	H	L	A	O	K
12	**H**	**A**	**L**	I	T	Z	S	Y	V	J	Q	A	G	W	N	P	L	U	M	H	X	D	B	O	F	K	R	E	C
13	**H**	**A**	**M**	G	K	R	W	T	O	A	Q	V	P	B	Z	X	Y	F	J	H	C	U	E	S	I	D	M	N	L
14	**H**	**A**	**N**	E	U	R	L	A	Y	P	W	M	O	S	D	I	T	J	G	X	C	K	N	B	Z	H	Q	F	V
15	**H**	**A**	**O**	S	V	H	F	X	D	O	C	R	P	M	U	K	Q	G	J	N	I	A	Z	L	B	Y	E	W	T
16	**H**	**A**	**P**	T	P	V	U	Q	L	N	R	O	W	Z	F	S	G	I	B	E	H	M	A	D	C	J	Y	X	K
17	**H**	**A**	**Q**	T	I	R	P	Y	Q	V	O	B	L	U	J	X	Z	H	D	F	C	W	A	K	G	S	M	E	N
18	**H**	**A**	**R**	Z	J	R	M	Q	U	P	N	O	B	Y	S	D	H	I	G	E	C	L	V	F	T	X	W	K	A

(The machine would go on making up more ciphers, but there is no more room here!)