3.4 Lesson 4 : Enigma cipher

The Enigma cipher machine was invented in 1915 bu two Dutch Naval officers. The German forces started in 1926 using a specially adapted military version to encrypt their communication. They continued to rely on the machine throughout the Second World War, believing it to be absolutely unkreakable.

Let's watch Dr Grim explaining how the Enigma machine worked https://youtu.be/G2_Q9FoD-oQ

The rotors

1) The classic Army issue Enigma machine used cipher wheels called **rotors** which could be taken out and changed. There were .rotors that the Enigma operator could chose from for the .slots in the machine. How many different ways are there of positioning 5 rotors in 3 slots? .....

.....

2) Navy cypher was harder to break. The Navy version of the Enigma had 8 rotors to pick from. How many different ways are there of positioning 8 rotors in 3 slots? .....

.....

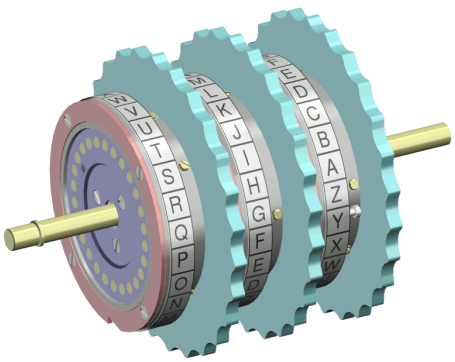
3) In how many different ways can you set the starting position of the rotors ? .....

.....

The ring settings and turnover points Each time a letter was pressed on the keyboard, the rotor on the (far left/middle/far right) would move around one place.

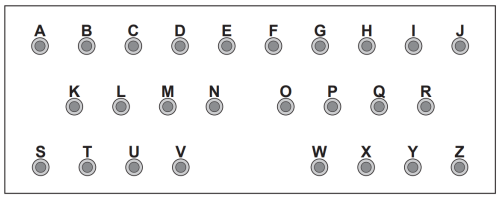
At one particular position it would kick the (far left/middle/far right) rotor forward one position. Then after a further complete revolution it would again kick the (far left/middle/far right) rotor forward by one position.

Likewise the (far left/middle/far right) at one of its positions would kick the left hand rotor forward by one position.



The plugboard was added to the Army issue Enigma machine to ..... the number of possible settings.

The Enigma machine had ..... cables that would be used to ..... pairs of characters.



Exercise 13 If you had 1 cable, in how many ways could the plugboard be set up? .....

.....

Exercise 14 In the video, Dr Grim shows that the number of ways to choose m pairs out of n objects is $\frac{n!}{(n-2m)!m!2^n}$. Evaluate the formula for $m = 10$ pairs out of $n = 26$ characters. In how many different ways can the plugboard be set? .....

.....

The number of settings of the Enigma machine is = number of ways of positioning 5 rotors in 3 positions

× number of different starting positions of rotors

× number of ways of connecting plugboard

=.....

=.....

Encoding/decoding using paper enigma Set Up :

- Make sure that the grey bars on the Reflector and the Input/Output cylinders line up; this shows the start position of your Enigma machine and lets you track the turnover positions of the rotors.
- Turn the rotors so that the three letters of your message key are in line with the grey bars.

For each letter in your message:

- Turn just the right-hand rotor one step towards you (so the letter in line with the grey bar becomes the next one alphabetically); make sure that the other rotors and the Input/Output cylinder stay still. You must do this before you read off the letter (even the first one!)
- Find the letter from your message on the Input/Output cylinder at the right-hand side, and trace the line from it through all three rotors, in to the reflector, out again back through all three rotors and into the Input/Output cylinder again. Write down the letter at which you end up.

For practice, try this message with Reflector B, rotor I, rotor II, rotor III, I/O with key A B C.

Ciphertext	A	E	F	A	E		J	X	X	B	N		X	Y	J	T	Y
Plaintext																	

Try also this message with rotors I, II and III, with key A B R (finish position at A C P).

Ciphertext	M	A	B	E	K		G	Z	X	S	G
Plaintext											

The flaw in the Enigma machine In https://youtu.be/V4V2bpZlqx8 Dr Grim explains the flaw the idea behind breaking the Enigma cipher.

About the movie "The imitation game"