THE ENSYFA MACHINE

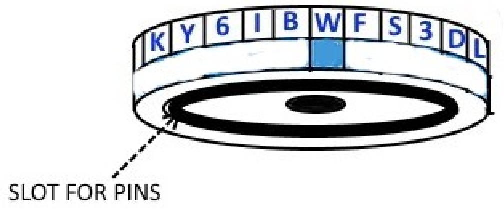
A wooden cryptography device using the principles of the ENIGMA machine

This device consists of a set of wooden wheels bearing substitution cipher alphabets around their circumference. The device is operated by hand to produce enciphered text which is practically impossible to decode without knowledge of the enciphering process and its components and settings. Cipher-only cryptanalysis of the code output, although theoretically possible, would be an extremely tedious, difficult and time-consuming process requiring some prodigious computer power to achieve.

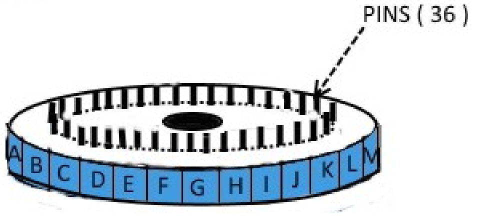
Components are as follows :

Shaft : 6 mm diameter wooden dowel

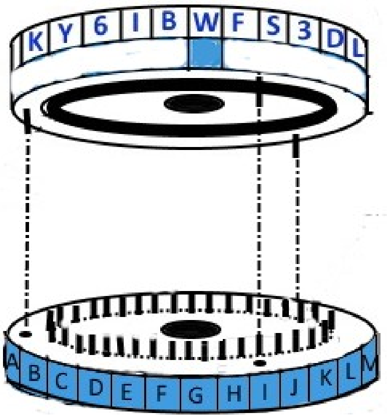
Rotor Bases : Each consisting of 2 x 55 mm diameter MDF discs, 6 mm thick
Alphabet Ring : 1 x 55 mm MDF disc.



ROTOR BASE – 2 DISCS GLUED TOGETHER WITH 5 mm DEEP CIRCULAR SLOT, 20 mm DIAMETER



ALPHABET RING – 1 DISC WHICH ATTACHES TO ROTOR BASE THROUGH 3 PINS.



THE ALPHABET RING CAN BE ATTACHED IN ANY OF 6 DIFFERENT ORIENTATIONS

Reflector Ring: 2 discs glued together with reflector lettering, one row for enciphering and one for deciphering.

Input Ring : 2 discs glued together with one row of letters for text input.

Examples of the letter rings for each are shown below :
Rotor Wheel Cipher letters

V	5	L	Y	U	H	F	2	Ø	W	D	6	Z	G	7	Q	E	S	M	4	P	O	T	R	I	B	3	1	9	8	X	A	K	N	C	J

Rotor Wheel Alphabet Ring

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	Ø	1	2	3	4	5	6	7	8	9

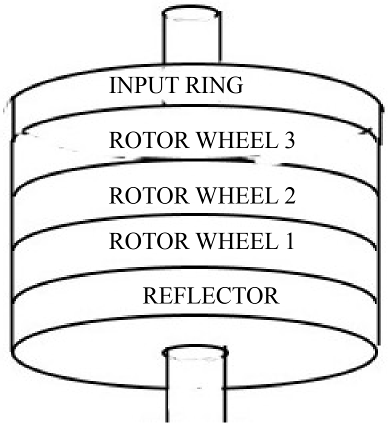
Reflector Ring

V	►	L	A	D	►	E	R	Z	F	Q	U	B	T	X	U	F	S	J	K	D	Z	K	V	E	Y	R	A	►	X	T	S	Y	Q	B	L

V	◄	L	A	D	◄	E	R	Z	F	Q	U	B	T	X	U	F	S	J	K	D	Z	K	V	E	Y	R	A	◄	X	T	S	Y	Q	B	L

Input Ring

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	Ø	1	2	3	4	5	6	7	8	9



To use the Ensyfa device, a set of rings is put onto the shaft. From bottom to top, these are the Reflector, three Rotor Wheels* and the Input Ring at the top.

* A minimum of 3, but more can be used as desired. More rotors gives greater security, but lengthens the time needed to encode the message. The Rotor Wheel sequence would be chosen according to a secret key. [See Notes]

OPERATION OF THE ENSYFA

There would usually be a set of 10 or more different Rotor Wheels, from which the operating set can be selected. Each of these has a detachable Alphabet ring which can be installed in 6 different positions on the Rotor Base. When the rotors have been assembled in the correct locations, the A on the Input Ring is aligned with the J on the Reflector Ring. The Rotor Wheels in between these must then be rotated so that a key letter sequence, eg K4X, is aligned in the same column as the Input A and Reflector J. The Ensyfa is then ready for enciphering the text message.

The first letter of the text is located on the Input Ring, and below it on Rotor 3 the Cipher character (blue) in the same column is read off. This Cipher character is then located on the Alphabet Ring of Rotor 3 (red) and the Cipher character in the same column on Rotor 2 is read off. These steps are repeated on Rotor 1 and the Red character on Rotor 1 is found. This will be located in the same column as a character in the Encoding line of the Reflector (blue).

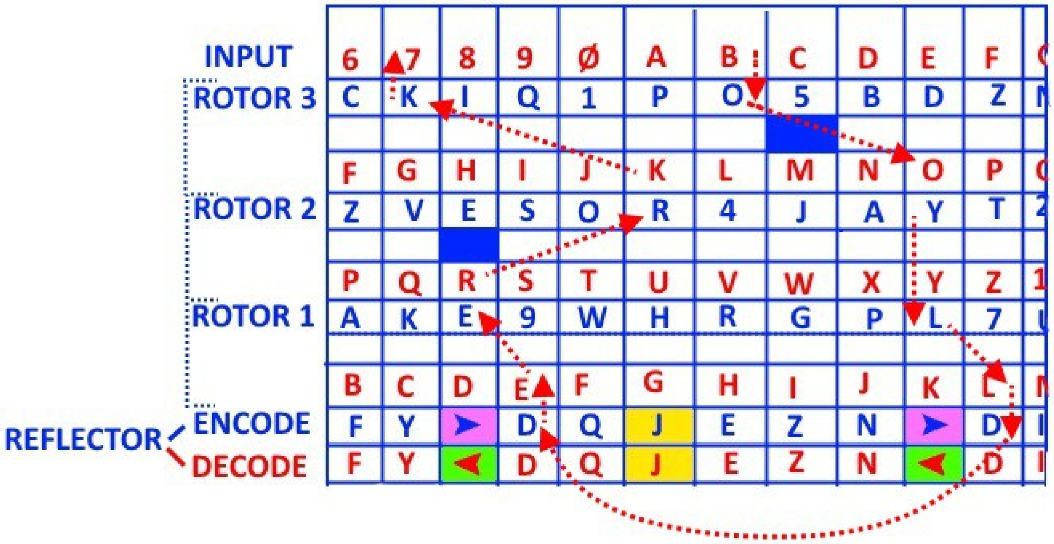
The Reflector has two entries for each letter (except J) and when the Encoding line is entered from Rotor 1, the whole Ensyfa assembly is rotated (keeping all the rotors aligned) to find the other location of the Encoding line letter. From there, the reverse path is followed back through Rotors 1, 2 & 3 to the Input Ring, where the final enciphered character for the plain text input is located.

The Reflector has a single entry for the letter J, which means that the plain text input letter will be enciphered as itself, by retracing the path back through the three rotors to the Input Ring. Also there are 3 ► arrows on the Reflector, which mean that instead of jumping to the same letter on the Encoding line, the jump is to the next ► character in the same direction.

Although this looks rather complicated, it is just equivalent to a single monoalphabetic substitution, which can be easily cracked by letter frequency analysis. To make cryptanalysis more difficult, it is necessary to step the rotors each time a letter has been enciphered, beginning with Rotor 1. The Rotors have a number of blue squares marked on them, these are used to indicate jumping of the higher Rotors. Whenever two adjacent rotors show blue squares in the same column, the higher Rotor jumps to the next blue square location. Further complexity can be introduced by stepping some of the rotors in the opposite direction. Obviously the more complex the stepping procedure, the longer it will take to encipher the text and the more the procedure will be prone to errors. This is the trade off for increased security.

DECIPHERING

When an enciphered message has been received, it is necessary to know the initial settings for the Rotor sequence, Alphabet Ring settings and Keyword used before it can be deciphered. If a Rotor stepping procedure was used, this must be known also. The Ensyfa wheels are set up with this information and each letter of the message is traced through the Rotors in exactly the same way as was done for the encipherment, with the one exception that the Decoding line of the Reflector ring is now used, reading in the reverse direction. When applicable, stepping takes place after each letter is deciphered in the same manner as for the encipherment.



INPUT	6	7	8	9	Ø	A	B	C	D	E	F	G
ROTOR 3	C	K	I	Q	1	P	O	5	B	D	Z	M
								■				
	F	G	H	I	J	K	L	M	N	O	P	Q
ROTOR 2	Z	V	E	S	O	R	4	J	A	Y	T	2
			■									
	P	Q	R	S	T	U	V	W	X	Y	Z	1
ROTOR 1	A	K	E	9	W	H	R	G	P	L	7	U
	B	C	D	E	F	G	H	I	J	K	L	M
REFLECTOR ENCODE	F	Y	➤	D	Q	J	E	Z	N	➤	D	I
REFLECTOR DECODE	F	Y	◀	D	Q	J	E	Z	N	◀	D	I

This diagram shows the setup of the Rotors with the keyword **PRH** in the **A---J** column. If the first letter of the plain text message is **B,** then the path through the Rotors & Reflector is shown by the red dotted lines. The output of the encipherment would be **7.**

If a message was being decoded and its first character was **7**, then the path through the rotors would follow the reverse path, except that the Decode line of the Reflector would be used. In this example the Decode line has the letter **D**, so the path jumps to the other location with the same letter, but if the reflector letter was **J**, the path would retrace back to the input letter. If an arrow is encountered on the Reflector, the path jumps in the direction shown to the next arrow.

NOTES

The security of this device is dependent on the secrecy of the Rotor sequences and Keywords, which must be exchanged between the sender and receiver. An example of a code setting is as follows :

ROTORS	ALPHA RINGS	KEYWORD
XQT	D3V	PRH

This would indicate that the rotor sequence (Top to Bottom) is XQT, the X Rotor has the Alpha ring A aligned with D on the Cipher ring, the Q Rotor has A aligned with 3 and the T Rotor has A aligned with V. The keyword in the A---J column is PRH.

With 3 rotors (selected from 15) this allows 2730 rotor sequences, 216 Alpha ring settings and 46656 Keywords, a total of 3,924,910,080 posible settings. While this is far too many to analyse manually, it is not too difficult for a computer to check each setting and decipher the code. The security can be enhanced by increasing the number of rotors, as shown in this table :

	3 ROTORS	**4 ROTORS**	**5 ROTORS**	**6 ROTORS**
Rotor sequences	2730	32760	360360	3603600
Alpha settings	216	1296	7776	46656
Keywords	46656	1679616	60466176	2176782336
Total	3.9×10^{9}	7.1×10^{13}	1.7×10^{17}	3.6×10^{20}

In addition, there are 36! (3.72×10^{42}) possible permutations of characters on each Rotor, and the stepping procedures must be known to the attacker. As long as none of this information is known to the attacker, the system is extremely secure against cryptanalysis, more so than the original German Enigma machine. The WWII codebreakers managed to crack the Enigma system only after years of work by many hundreds of people, and because they were in possession of captured machines. Although rotor-type enciphering machines are no longer considered safe against cryptanalysis for secret military purposes, they are still able to provide a high level of security against casual attackers.