Dyson Foundation Activity Day: Enigma

Introduction

The Enigma machine was an electromechanical encoding device used by German military branches during the Second World War. It was invented by Arthur Scherbius, and consisted of a keyboard, lampboard, and scrambling circuit. The machine was capable of scrambling a letter in one of 105,456 possible ways, and with later iterations came additional complexity leading to literally hundreds of billions of permutations. In 1938, before Alan Turing and the codebreaking effort at Bletchley Park, a group of mathematicians working secretly in Poland build a machine to break the Enigma code: The Cryptological Bomb, or 'Bomba'. As a result, Polish intelligence services were able to read secret German military codes before they were invaded in 1939.

The Dyson Foundation sponsored a University of Cambridge fourth year project aiming to recreate this piece of forgotten history. The project had mixed successes: the electrical circuit and proof of concept were achieved, but unfortunately the final machine was not finished as hoped due to a mechanical failure.

Dyson Foundation Day Activity: Enigma

While interesting, the complex nature of the Polish methods meant that running an activity based around the Bomba itself would be infeasible in a 45 minute session with secondary school children. Furthermore, it is a prerequisite of any work on the Bomba to have a detailed understanding of the operation and characteristics of Enigma. As such, it was decided that an activity should planned around Enigma, with a focus upon looking at the reflection property of the Enigma machine which the Poles exploited.

In the session, students would use Enigma wiring diagrams, fitted to moveable rotors, to trace the electrical signal throughout the encryption process. It aimed to consider the basic operation of Enigma, the behaviours this resulted in (reflection) and some brief discussion of how these might be used in codebreaking.

An Enigma machine has four key components: input keyboard, output lampboard, rotors, and stecker or plug board. The plugboard switches pairs of input letters, drastically increasing the complexity of the encryption. For the purposes of this activity it will be ignored and so will not be referenced further in this document. To encode a message, an operator would type each letter out on the input keyboard. Pushing a key caused the rotor mechanism to advance one position, changing the cipher for every letter. At the bottom of each key depression, an electrical contact formed, sending the signal through the series of rotors, and into the reflector, before returning once more through the rotors and then

illuminating a bulb on the lampboard corresponding to the output letter. Figure 1 shows a wiring diagram for this process.

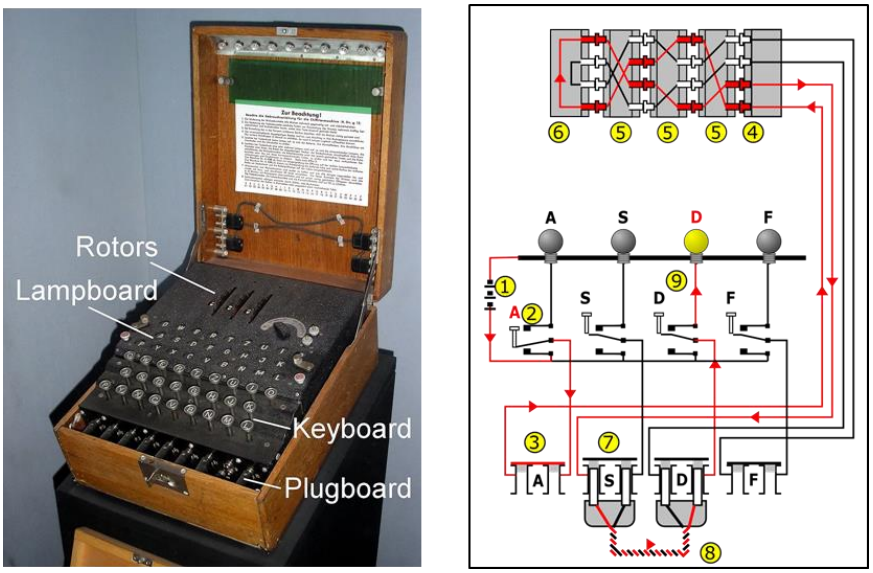

Figure 1: Labelled Enigma depiction and simplified wiring diagram (source: Wikipedia[i])

The models used for the activity mimicked the rotary part of Enigma. They were made from surplus 3D printer reels, machined to a smooth finish and mounted on PVC piping. The reflector rotor was rigidly fixed to the PVC shaft, whilst the other 3 rotors could be moved. They were also removable so that all 105,456 permutations of the basic Enigma were achievable with this model.

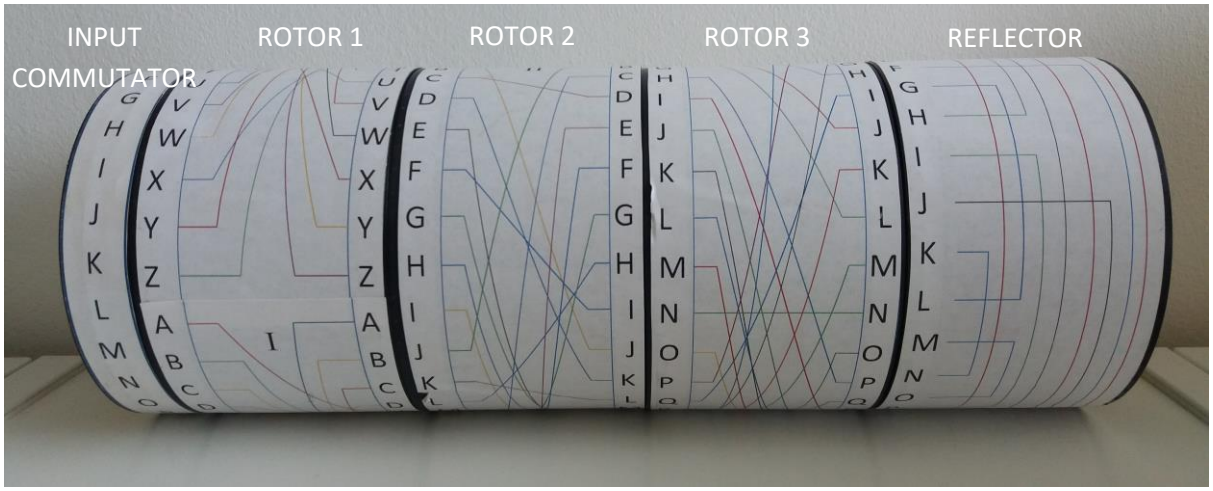

Figure 2: Engima rotor model

For the activity, students worked in pairs, using the model Enigma rotors to solve a few simple encoding tasks. The first task aimed to establish the reflection property of Enigma which allowed it to be self-decoding. In this task, students followed the wiring connections for four different input letters. It would transpire that the inputs chosen were all the output for another input (see Activity 1 on page 5) e.g. if A enciphers to N, then N enciphers to A. Students were encouraged to discuss why this allowed Enigma to be self-decoding and why it is useful to have a combined encoding/decoding machine, but also how this might make the machine vulnerable to codebreakers. To build upon this, in the second activity, the students enciphered/deciphered their names, turning the rotors with each letter inputted like a real Enigma machine would. This gave them a sense of how the mechanism worked, and visibly demonstrated the moving electric circuit as well as confirming the reciprocity of Enigma. Students discussed why using rotors changed the circuitry for each letter in the message, and why this in turn changed the cipher. As a group, we then considered why this makes Enigma impossible to break by traditional hand methods and hence why machine ciphers were adopted before the Second World War.

The final exercise had the students using the model Enigmas to decipher a series of short codes. The codes turned out to be the names of famous Second World War codebreakers, including the Polish mathematicians who built the Cryptological Bomb. This led into a brief explanation about how the Polish Bomba machine used the reflection property of Enigma to find the daily Enigma settings. One of the names listed in the final activity was Tommy Flowers. Surprisingly, whilst some of the other code breakers were identified by the students, nobody had heard of either Flowers or Colossus, the first programmable machine. Colossus was designed by Flowers, who worked at Bletchley Park during the war, to break the Lorentz cipher used by the German high command. The students discussed the benefits of a programmable codebreaking machine compared to a purpose built machine like the Polish Bomba, which became obsolete every time a new version of the Enigma machine was utilised or a new operational procedure developed. This led into a final discussion about how the modern computer has made custom encoding machines vulnerable to decryption. Students discussed how encoding can now be achieved by computing machines such as small hand held electronics and why society might be interested in this application for data privacy.

A completed copy of the handout used to guide students through the activity can be found on pages 5 and 6.

Reflection on the activity

The activities overall were a success, although students were slower than expected at using the model Enigma machines, as the initially some found following the complex wiring diagrams challenging. However, by the end of the session, all students had a basic

knowledge of what Enigma was and how it worked, and why it was vulnerable to codebreakers. They also had practised or considered some of the skills and activities that might be needed from a working electrical or information engineer such as using wiring diagrams and reviewing information security. Upon later discussion with some of the students, it transpired that many had not considered the breadth of projects that an electrical or information engineer may encounter, and few had thought about how extensively electrical and information engineering now impacts our society in the example of data protection, historically, and in many other ways.

James Dyson Foundation Activities Day: Enigma

Activity One

Ensure the Enigma rotors are aligned (A-A-A-A-A connected etc.). Find the output of each rotor stage for the following inputs:

Input	Rotor I	Rotor II	Rotor III	Reflector	Rotor III	Rotor II	Rotor I	Commutator
A	***E***	***S***	***G***	***L***	***F***	***W***	***N***	***N***
E	***L***	***H***	***P***	***I***	***Q***	***Q***	***H***	***H***
H	***Q***	***Q***	***I***	***P***	***H***	***L***	***E***	***E***
N	***W***	***F***	***L***	***G***	***S***	***E***	***A***	***A***

What does this tell us about Enigma? ***Reciprocity: when A goes to N, N also goes to A. This is because the rotor wiring forms a complete electric circuit: if A is +ve direction, then N is –ve direction.***

Activity Two

An Enigma machine has a keyboard to enter the message you want to encode. An array of light bulbs indicates what each letter has been encoded to. Each time a key on the keyboard is pressed, a mechanism moves the first rotor by one place. **For this activity, before enciphering each letter, move *Rotor I* one place forwards** (e.g. for the first letter, the left hand side of Rotor 1 will have B next to letter A on the input ring).

You should read outputs from the input commutator ring, not from rotor 1.

e.g.

Input	Rotor I	Rotor II	Rotor III	Reflector	Rotor III	Rotor II	Rotor I	Commutator
M	W	Y	Q	E	P	U	I	H
I	N	H	P	I	Q	Q	S	Q
K	W	N	N	K	U	H	B	Y
E	V	G	C	U	W	M	H	D

Encipher your name using the Enigma rotors: H Q Y D (MIKE)

Now move the rotors back to the starting position and put your encoded message through Enigma. The result should be your name. Why is this? ***Reflector allows Enigma to be self-decoding (complete circuit).***

Activity Three

Below are seven codes. Turn your Enigma rotors so that they are aligned (A-A-A-A-A etc.). **For this activity, before enciphering each letter, move *Rotor I* one place forwards** (e.g. for the first letter, the left hand side of Rotor 1 will have B next to letter A on the input ring).

Enigma Code	Deciphered Message
MFLQWM	***Henryk (Zygalski)***
HTFXGP	***Marian (Rejewski)***
YLFEZP	***Gordon (Welchman)***
ZLGAW	***Tommy (Flowers)***
HTCXI	***Mavis (Batey)***
FOZP	***Alan (Turing)***
CFEDU	***Peter (Twinn)***

Appendix: Enigma Wiring Connections

Letters	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
Rotor I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
Rotor II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Rotor III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
Refl. B	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

References

[i] https://upload.wikimedia.org/wikipedia/commons/thumb/3/3e/EnigmaMachineLabeled.jpg/220px-EnigmaMachineLabeled.jpg

https://upload.wikimedia.org/wikipedia/commons/thumb/5/53/Enigma_wiring_kleur.svg/725px-Enigma_wiring_kleur.svg.png