PERTH MODERN SCHOOL

Exceptional schooling. Exceptional students.

Course: Methods Year: 11

Student Name: ____________________ Teacher Name: ________________

Date: 10/02/23 – 17/02/23

Task Type: **Investigation**

Reading Time: **5 minutes**

Working Time: **40 minutes**

Number of Questions: **TBA**

Materials Required: CAS calculator (ClassPad) and one double-sided A4 page of notes (no take-home section)

Standard Items: Pens (blue/black preferred), pencils (including coloured), sharpener, correction fluid/tape, eraser, ruler and highlighters

Special Items: Drawing instruments, templates, notes on one unfolded sheet of A4 paper, and up to three calculators approved for use in the WACE examinations

Marks Available: **TBA marks**

Task Weighting: **10 %** (year)

Formula Sheet Provided: **No** (formulas will be provided on Page 2)

Note: All questions worth more than 2 marks require working to obtain full marks.

INVESTIGATION 1: COUNTING TECHNIQUES
Alan Turing and the Enigma Machine

BACKGROUND

Alan Turing was a British mathematician who was born in 1912. By the age of 22, he was nominated to be a fellow of King's College Cambridge. Two years later, he published a paper titled *On Computable Numbers*, in which he conceptualised the first universal **computer**.

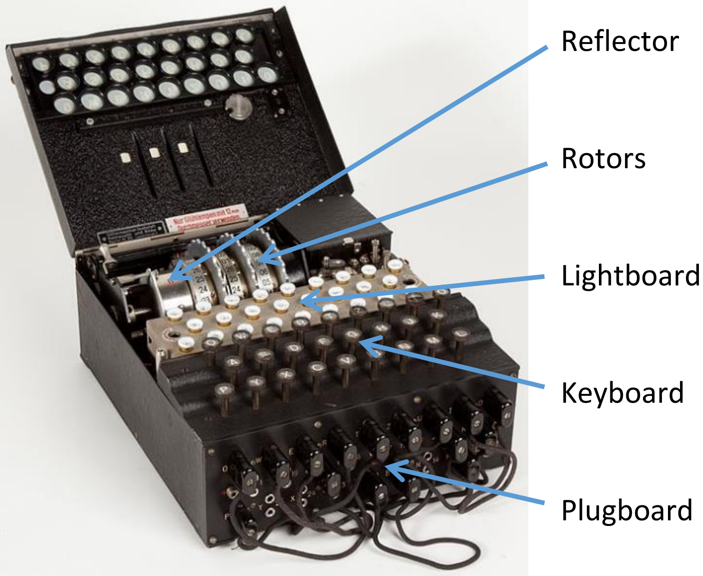
In 1950, Turing wrote another paper titled *Computing Machinery and Intelligence*, where he both predicted that computers will eventually think like **humans** and proposed the **Turing Test**. If a person asks a computer and a human a series of questions and is unable to **distinguish** them based on their answers, then the computer has **passed** the Turing Test and can be considered to have **artificial intelligence**.

Turing is considered to be the **'father of computing'** for his visionary contributions to the field. Time Magazine listed him among their *100 Most Important People of the 20th Century*. Numerous books and several movies have been dedicated to Turing, including the 2014 movie *The Imitation Game*, where he is played by Benedict Cumberbatch.

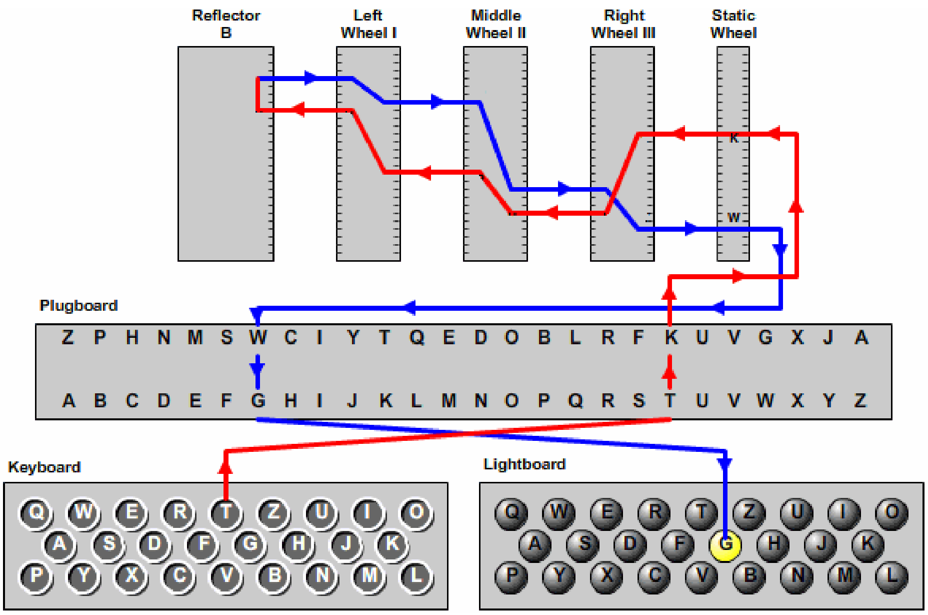
Turing is also famous for his pivotal role in **World War II** whereby he led a British intelligence team in efforts to **decipher** highly encrypted radio messages sent by the German military. These messages were encrypted using devices known as **Enigma machines**. The first version was invented in 1923 by German electrical engineer **Arthur Scherbius**.

There are nearly **159 quintillion** possible encryption settings to the main Enigma machines used by Germany during the War, which made it extremely difficult to decipher their messages. The messages were further secured because the German military changed their encryption settings **daily**.

Germany thought the Enigma encryption was **unbreakable** and were dependent on the machines to encrypt their radio communication. Their extensive use of Enigma machines made deciphering their messages a **top focus** for Britain's efforts.



HOW THE ENIGMA MACHINE WORKS



Enigma machines are **electromechanical** devices, designed to both **encrypt and decrypt** messages. The key features of the main version used by Germany during the War are:

- **Keyboard**: Has the **standard alphabet** for input. When a key is pressed, it mechanically **sequences** the rotors, then **transmits** an electrical signal.
- **Plugboard**: Consists of 26 sockets – one for each letter. **Ten wires** are plugged into ten pairs of sockets to **substitute** the connected letters for encryption, with six letters **unchanged**. For instance, in the diagram above, T changes to K (and K correspondingly to T), while I does not change. The plugboard can be **rewired** to change the **encryption settings**.
- **Rotors**: Each rotor has 26 electrical contacts on each side and 26 internal wires that connect between the contacts on each side in a scrambled arrangement. The rotors **connect** to each other via the contacts (see right) to transmit the electrical signal along a **scrambled pathway**, effectively **substituting** letters for encryption.

  The rotors sequence with **each keystroke** similarly to the hour, minute and second hands of a **clock**. This **constantly changes** the encryption setting by changing how the rotors connect, thus providing the highest level of encryption – **polyalphabetic substitution**. This means that each input letter will not always generate the same output letter, so it **cannot** be deciphered using **direct substitution**.

  The rotors can be **manually** rotated to configure the **initial** encryption settings. The machine uses **three rotors** out of a **set of five** rotors, so these can also be **swapped** around to introduce **more** encryption settings.
- **Reflector**: Consists of 26 electrical contacts and 13 internal wires connecting them in pairs. It **redirects** the signal back through the rotors and plugboard to the lightboard, via a second pathway. The reflector was incorporated to **simplify decryption** – it created **reversible** electrical pathways so typing an encrypted letter generates the original letter (with the same encryption setting).
- **Lightboard**: Lights up to indicate the **output letter**, for as long as the key is held. The output needs to be written down.

While Enigma machines are complicated in design, the operation is simple:

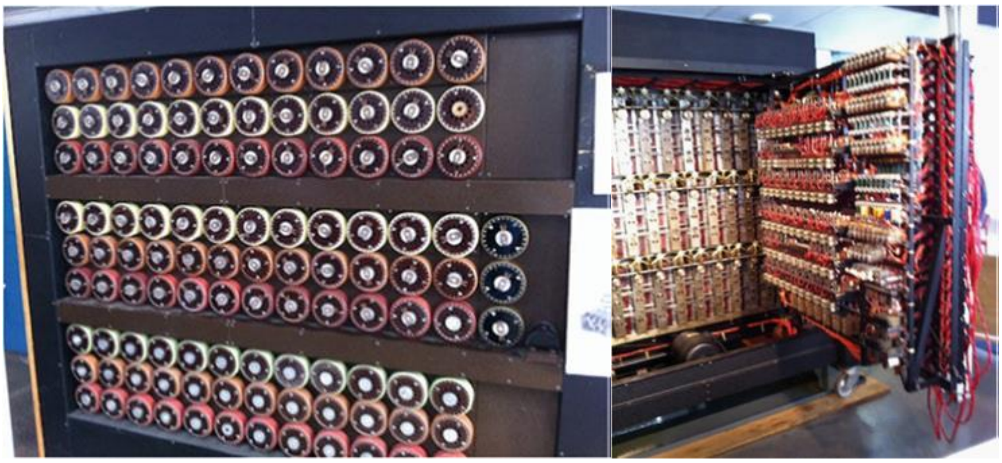
1. **Encryption**: Configure the initial settings (**rotors** used, rotor **order**, rotor **positions** and **plugboard** wiring), type in the message and record the encrypted message.
2. **Decryption**: Configure the **same initial settings**, type in the **encrypted** message and record the original message.

BREAKING THE CODE

In 1935, **Poland** was the first to break Enigma encryptions (with access to Enigma machines), after they pre-emptively began deciphering Germany's radio messages in 1928. However, this was before the German military added the **plugboard** to the Enigma design. Poland was defeated in 1939, at the beginning of the War, but shared their intelligence with **Britain** (and France), who assembled a team of **top mathematicians** and cryptologists in Bletchley Park to decipher Germany's upgraded encryptions.

Turing and his team also had access to Enigma machines, allowing them to study its **design**. While the **reflector** simplified encryption and decryption, it also meant that no letter could generate **itself** as the encrypted output. This allowed the team to match expected phrases, such as *wetterbericht* (*German: weather report*), to strings of letters in the encrypted message, providing **starting points** for analysis.

Turing worked closely with another mathematician, **Gordon Welchman**, to design an electromechanical computer, called the **Bombe** (see below), to help with their deciphering efforts. The Bombe was **not** a universal computer with universal functionality and did **not** decipher Enigma messages. However, it did **eliminate** encryption settings very quickly and identify **potential** settings for the British to further investigate. **12,000 people** worked 24 hours a day, 7 days a week with 200 Bombes to determine Germany's daily encryption settings and decipher their messages.



Information obtained from these operations was absolutely **top secret** and codenamed **Ultra**. Ultra intelligence had to be used extremely carefully to counter Germany's operations without **alerting** them of Britain's breakthrough. The Ultra operations were so classified that they were not publicly known until **1974**, after the publication of *The Ultra Secret*. As described by **Winston Churchill**, the Ultra team were *the geese that laid golden eggs but never cackled*. They are credited for helping the Allied forces defeat Germany and shorten World War II by 1-2 years, saving **potentially millions** of lives.

INVESTIGATION

The Original Enigma Machine

Question 1

The original Enigma machine has three rotors, each with 26 possible positions.

a) How many ways can you order or arrange the three rotors?

b) How many ways can you configure each rotor arrangement (using their positions)?

c) Hence, how many encryption settings are there in total?

The Military Enigma Machine

Question 2

The Enigma machine used by the German military uses three rotors out of an available set of five rotors, each with 26 possible positions.

a) How many ways can you order or arrange three rotors from the set?

b) How many ways can you configure each rotor arrangement?

c) Hence, how many encryption settings are there in total for the rotors?

Question 3

The military Enigma machine also had a plugboard with 26 letters and 10 wires to pair them.

a) How many encryption settings are there for the rotors (from above).

b) How many ways can you configure the plugboard?

i) How many ways can you choose 20 sockets from 26 sockets?

ii) How many ways can you pair up 20 sockets?
Hint: The order of the 10 pairs ***and*** *the 2 sockets in* ***each*** *pair do not matter.*

iii) Hence, how many plugboard configurations are there in total? Express your answer in scientific notation to 10 significant figures.

c) Hence, how many encryption settings are there in total for the military machine? Express your answer in scientific notation to 10 significant figures.

Question 4

The German military later added three more rotors to their set to have eight rotors in total. Calculate the number of possible encryption settings for the upgraded machine, showing all working. Express your answer in scientific notation to 10 significant figures.

Optimising the Plugboard

Question 5

The German military used ten wires to generate almost 151 trillion plugboard configurations. However, different numbers of wires, ranging from no wires to 13 wires, can be used to pair up the sockets. Explore the number of configurations for different numbers of wires, and hence determine the number of wires that will generate the most configurations. Show working for at least five different numbers of wires.
Hint: To speed up your exploration and calculations, expand out your first calculation, then look for a way to simplify and generalise it (unless you already simplified it in Q3bii).

Additional Information

Recommended

For further information and explanations on the Enigma machine, check the links below:

https://www.youtube.com/watch?v=G2_Q9FoD-oQ

https://brilliant.org/wiki/enigma-machine/

Optional

For further information on how Alan Turing and his team were able to break Enigma encryptions using logical reasoning and automated computation, check the video below:

https://www.youtube.com/watch?v=V4V2bpZlqx8

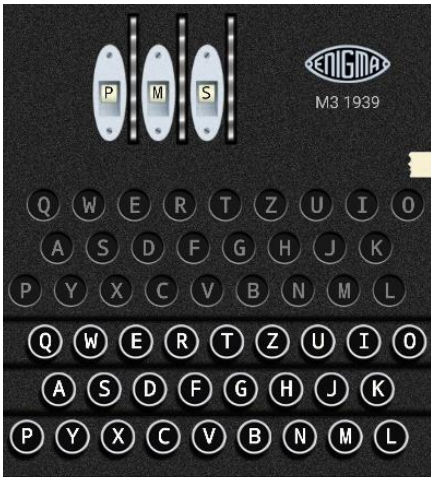
You can try the Enigma machine using the app below:

https://play.google.com/store/apps/details?id=uk.co.20franklinheath.enigmasim&hl=en

Try decrypting the message below using these settings:

- Enigma Model: M3 1939
- Reflector: B
- Wheel Number: III, I, IV
- Ring Setting: 01, 01, 01
- Plugboard Pairs: KC, GM, JP, LZ
- Rotor Setting: P, M, S

UUESK DHKYF YXSMV DSNCK CEKXQ IFKIT KMY


P
M
S
ENIGMA
M3 1939
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L
Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L