The Enigma Machine

In this Kata, we are going to take a Test Driven Development (TDD) approach to creating our own digital encryption machine that simulates the inner workings of the Enigma Machine; Most profoundly known for its usage throughout World War II where confidential messages were sent without fear of being understood by anyone intercepting the message.

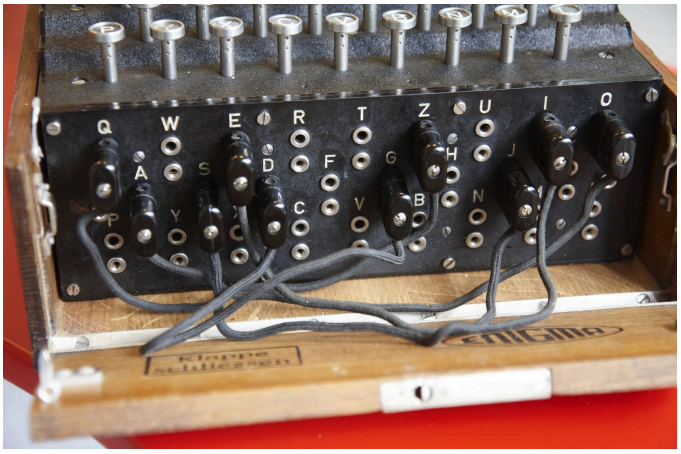
Due to the way the Enigma Machine works, it is a perfect candidate for using TDD during this exercise. The Enigma Machine has several components that individually appear to be simplistic - however, combining all these components resulted in a powerful encryption device that many doubted it would ever be broken.

Keyboard / Lightboard (Input and Output)

Operating the Enigma Machine was achieved by using the Keyboard. A user would type the unencrypted character into the keyboard and the decrypted letter would light up on the Lightboard. (e.g. Based on the configuration - a user can type the letter ‘F’ and the letter ‘K’ lights up on the Lightboard)

Plugboard

The plugboard, located at the front of the Enigma Machine allows the operator to route single characters of the alphabet to different characters. This was achieved by connecting wires between two characters on the plugboard. (e.g A wire connecting ‘T’ and ‘Z’ would mean a user could type ‘T’ on the keyboard and results in the plugboard returning the letter ‘Z’)



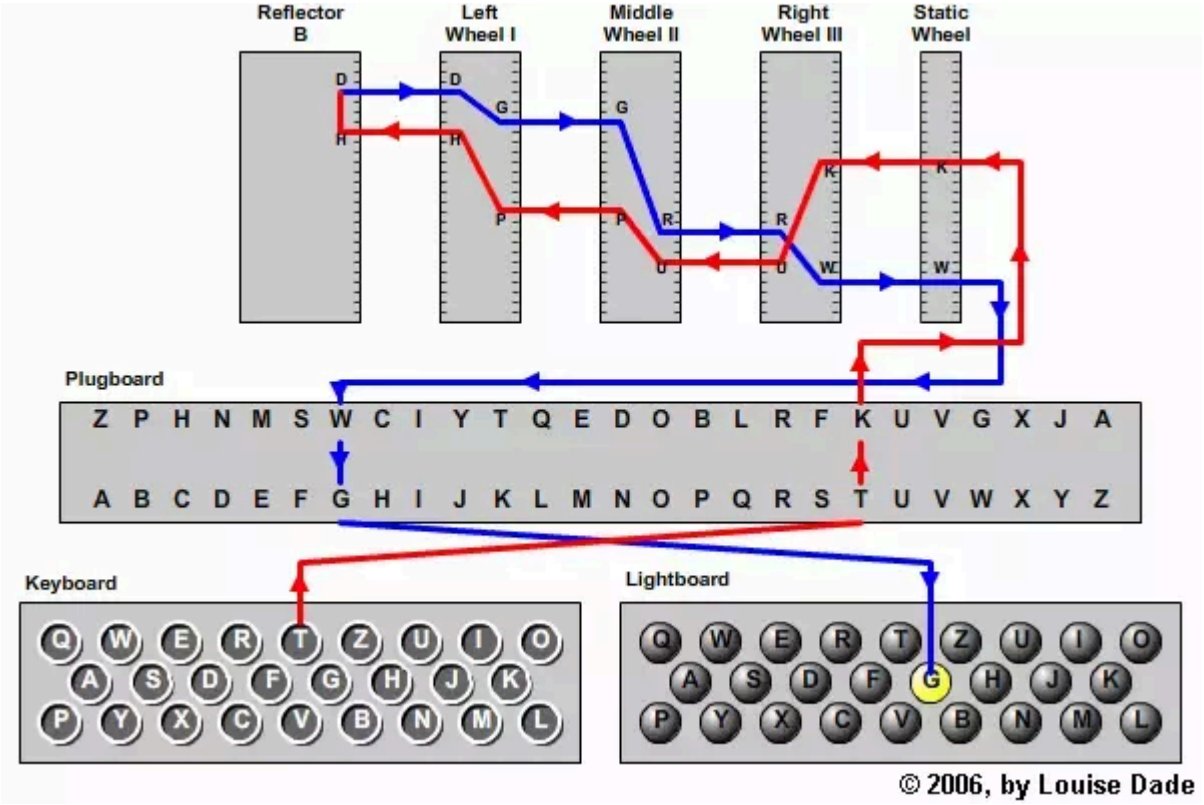
Rotor

Each Enigma Machine houses a minimum of 3 rotors. The rotor mechanism is by far the most important component of the encryption device and adds quintillions of possible permutations for encrypting a message. The rotor is a wheel that has 26 inputs and 26 outputs. Similar to the plugboard, each of the inputs on a rotor are mapped to a corresponding output.

When the user inputs a character from the keyboard, this causes a mechanical arm to rotate the first rotor to the next character. A rotor has a configurable notch that can be positioned at any of the 26 positions on the wheel. When a notch is encountered on a rotor, the rotor to the left is also rotated a single position. This is similar to how a car odometer works when tracking mileage.

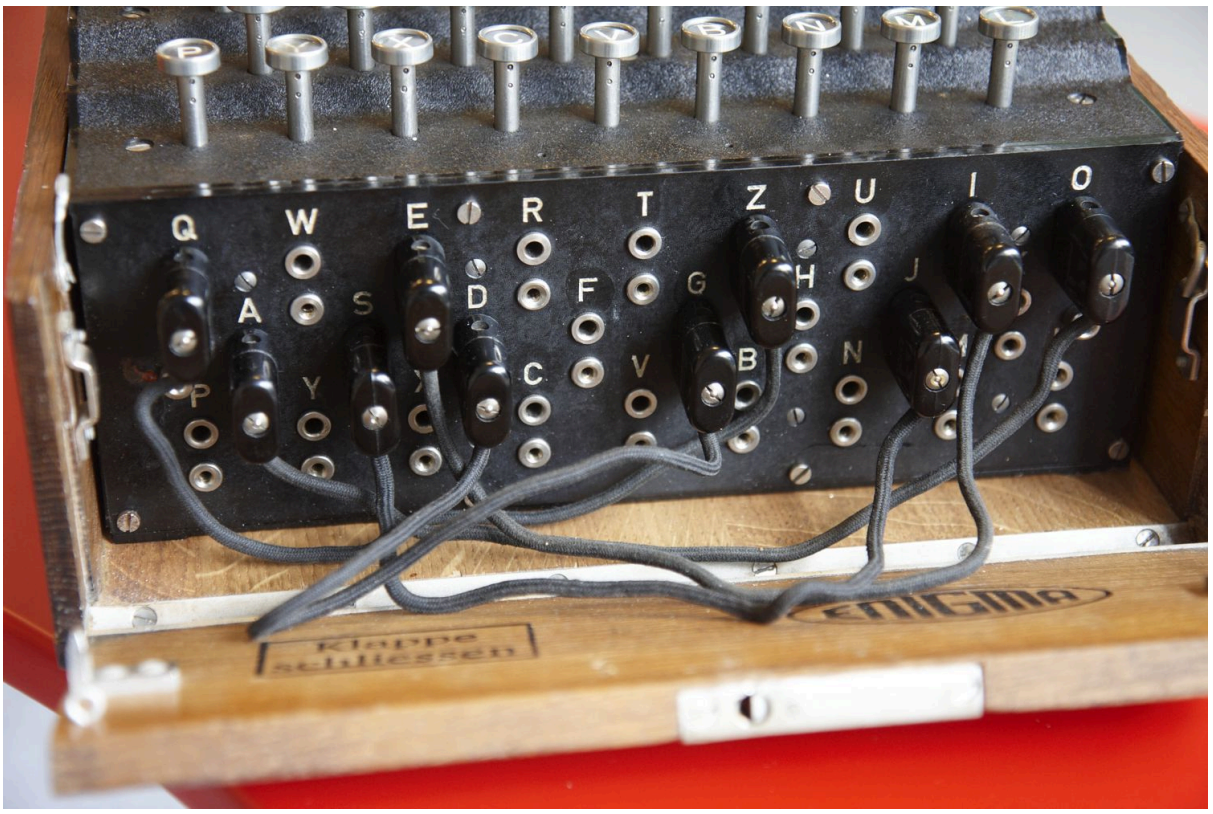
Reflector

At the end of the three or more rotors in the enigma is a component called the reflector. The reflector is a static device that has a fixed configuration. The image below shows how a single character being pressed on the Keyboard and the path it takes through the Enigma machine to result in an encrypted letter being returned on the Lightboard.



The Enigma Machine: Plugboard (Part 1)

The plugboard consists of 26 inputs which each have an associated letter. When joining two inputs together via a wire, this would result in the letters being switched round. (e.g. If the letter ‘A’ was mapped to ‘T’, when entering the letter ‘A’ then the output would be ‘T’).



A standard configuration for the Enigma's machine was to use up to a maximum of 10 wires to couple characters on the plugboard. When utilising all of these wires, only 6 characters would still be mapped to their original character.

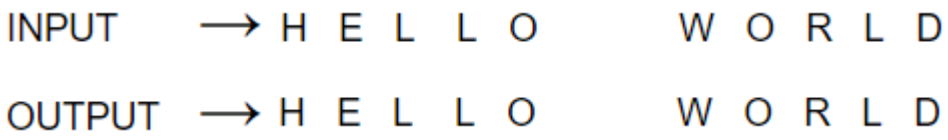
As part of this first Kata, we are going to first allow a configuration to be set and finally use the configuration to encrypt the users input.

The requirements of the plugboard are as followed:

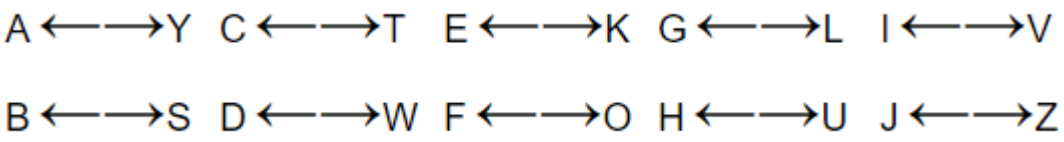
1) When no configuration has been provided, the default behaviour is to return the same character that was entered.
   An input of 'A' would result in an output of 'A'.
2) Successful configurations
   A configuration with a wire joining 'A' and 'B', an input of 'A' would result in an output of 'B'. An input of 'B' using the same configuration shall result in an output of 'A'.
3) Invalid configurations shall be denied:
   - More than 10 wires being used
   - Only one end of the wire being inserted into the plugboard
4) Implement the processing of a single character through a successfully configured plugboard

Test Scenarios:

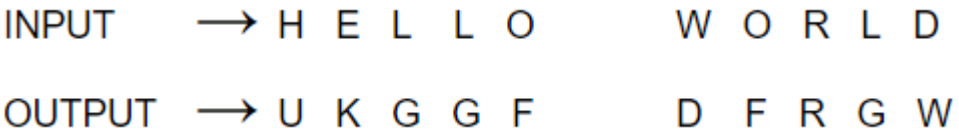
No Plugboard configuration:



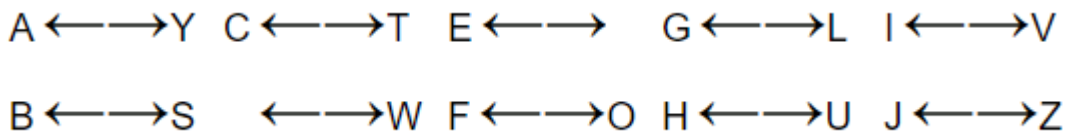
Valid Plugboard configuration:



When processing an input of ‘Hello World’ ’through a plugboard with the above configuration, the output will be as follows:

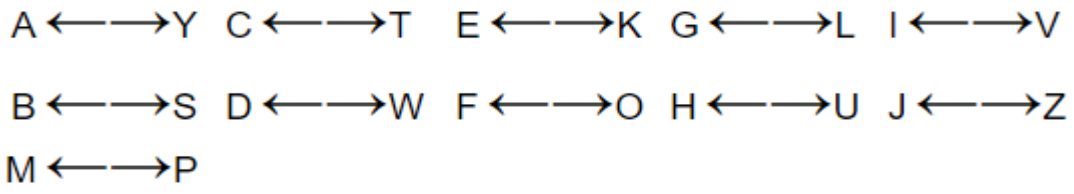


An error shall be returned when attempting to configure the Plugboard with the following wire pairings:



This is due to the letters ‘E’ and ‘W’ not having both ends of the wires being connected to the Plugboard.

An error shall be returned when attempting to configure the Plugboard with the following wire pairings:



This is due to the Plugboard exceeding the maximum of 10 wires.

Mathematical analysis. Combining three **rotors** from **a** set of five, **each** of the 3 **rotor** setting with 26 positions, and the plugboard with ten pairs of letters connected, the military **Enigma** has 158,962,555,217,826,360,000 different settings (nearly 159 quintillion or about 67 bits)

A ⟷ Y

B ⟷ S

C ⟷ T

D ⟷ W

E ⟷ K

F ⟷ O

G ⟷ L

H ⟷ U

I ⟷ V

J ⟷ Z

M ⟷ P

INPUT ⟶ H ⟶ **| 0 | 0 | 24|**

INPUT ⟶ E ⟶ **| 0 | 0 | 25|**

INPUT ⟶ L ⟶ **| 0 | 0 | 26|**

INPUT ⟶ L ⟶ **| 0 | 1 | 0 |**

INPUT ⟶ O ⟶ **| 0 | 1 | 1 |**

…

INPUT ⟶ H ⟶ **| 0 | 1 | 24|**

INPUT ⟶ E ⟶ **| 0 | 1 | 25|**

INPUT ⟶ L ⟶ **| 0 | 1 | 26|**

INPUT ⟶ L ⟶ **| 0 | 2 | 0 |**

INPUT ⟶ O ⟶ **| 0 | 2 | 1 |**

…

INPUT ⟶ H ⟶ **| 0 | 26| 24|**

INPUT ⟶ E ⟶ **| 0 | 26| 25|**

INPUT ⟶ L ⟶ **| 0 | 26| 26|**

INPUT ⟶ L ⟶ **| 1 | 0 | 0 |**

INPUT ⟶ O ⟶ **| 1 | 0 | 1 |**