Jackson Dunnigan

How To Use The Enigma Machine

Description

The enigma machine was an encryption machine used by the nazis in WWII to cipher messages. At the time, it was the most sophisticated encryption method ever made. It's comprised of 3 rotor slots on the front which all can contain a different rotor. There was 8 different rotors that were used in these slots and they can be swapped into different positions. There is also a plugboard on the front of the machine which can swap 2 letters when you input them. If you wish to learn this in more detail refer to this video https://www.youtube.com/watch?v=ASfAPOiq_eQ

How it encrypts a message

The rotors

The enigma machine encrypts a message by shifting your inputted letter via rotors. A rotor is comprised of the alphabet on one side and a randomly scrambled version of the alphabet in the other. When you input a letter, the signal goes through the first rotor and changes the letter to a random different one. For example: if you clicked "J" on the keyboard, it's the 10th letter of the alphabet. So it will be converted to the 10th letter on current rotor of the enigma machine. If "Q" was the 10th letter, on the rotors output side, "Q" will be transferred to the next rotor and the process repeats with the second rotor. After the signal goes through all the rotors, it gets reflected and goes back through the rotors again in reverse. The catch is, after every letter is clicked the entire machine changes its settings making it more difficult to crack.

The roots

When you view an enigma machine you see 3 letter along the top of the rotors, these are the roots. They are counted as 0 when encrypted. So as earlier stated, "J" is the 10th letter of the alphabet so it will be 10 letter from whatever the root is. The roots can all be changed into each letter of the alphabet further scrambling the possibilities. After every click, the root on the left most rotor shifts by one, after the first rotor does a full rotation, the second rotor shifts by one. After a full rotation of the second rotor, the third will rotate by one. This makes the machine more difficult to decrypt.

The Plugboard

On the front of the enigma machine there is many wires that connect two different letters on the alphabet. This is the plugboard. It lets you swap letters when inputted. For example if you input “J” and it’s connected to “Y” on the plugboard, it will so through the machine as if it was “Y” instead of “J”.

How to Use the Program

Encrypting

Before you encrypt your message, write down all 3 rotor roots, the rotors selected in every slot and each plugboard swap you’ve chosen. After that type in your message in and the ciphered version should appear in the output slot on the top left (refer to the image below). Click the “reset rotors” button and your settings will be converted back to what you set them to. Now you can type in your new message with these settings to decrypt it.

Decrypting

To decrypt a message, you input the encrypted message on the same settings that you encrypted it with. Input the encrypted message after you click reset and you should get your original message in the output. Now try decrypting it on different settings, you won’t get the right message. You can only get the right message if you have all correct settings. That’s what makes this so complicated. Aswell, There is over 15,000,000,000,000,000,000 combinations so no wonder it was viewed as unbreakable.