THE UNIVERSITY OF KARACHI

NAME: MUHAMMAD WAQAR.

CLASS: SEC-A BSCS (5TH) 3rd EVENING.

SEAT NO: EP-1549037.

SUBJECT: THEORY OF COMPUTER SCIENCE.

ASSIGNMENT: AUTOMATA (LAB).

SUBMITTED TO: MS FAIZA.

DEPARTMENT OF COMPUTER SCIENCE (UBIT)

ENIGMA MACHINE (SOFTWARE APPLICATION)

Abstract:

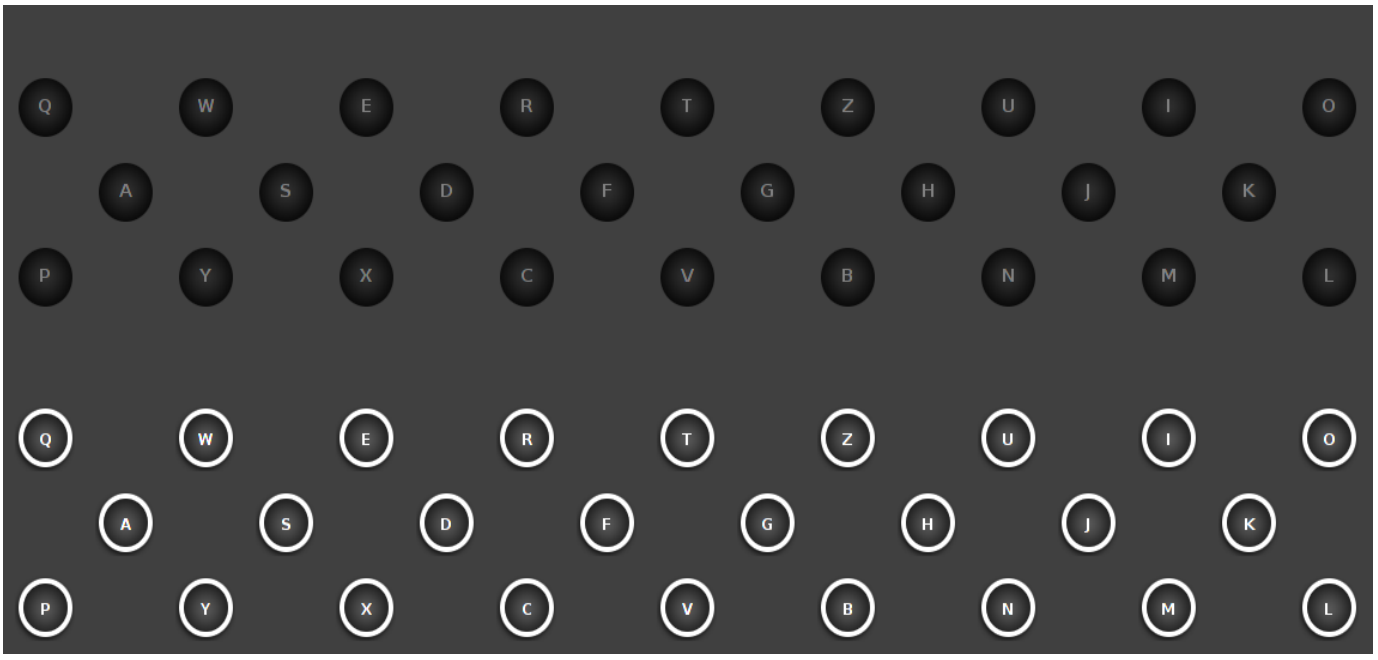
Enigma was invented by the German engineer Arthur Scherbius at the end of World War I. Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II. Several different Enigma models were produced, but the German military models, having a plug board, were the most complex. Japanese and Italian models were also in use.

Enigma machine which is a German Encryption machine which is used in World War II. Germans used enigma machine to send secret message to his Armed Forces. Enigma machine firstly has one standard keyboard, plug board, reflector (lamp board), 3 rooters.

Components of the Enigma machine:

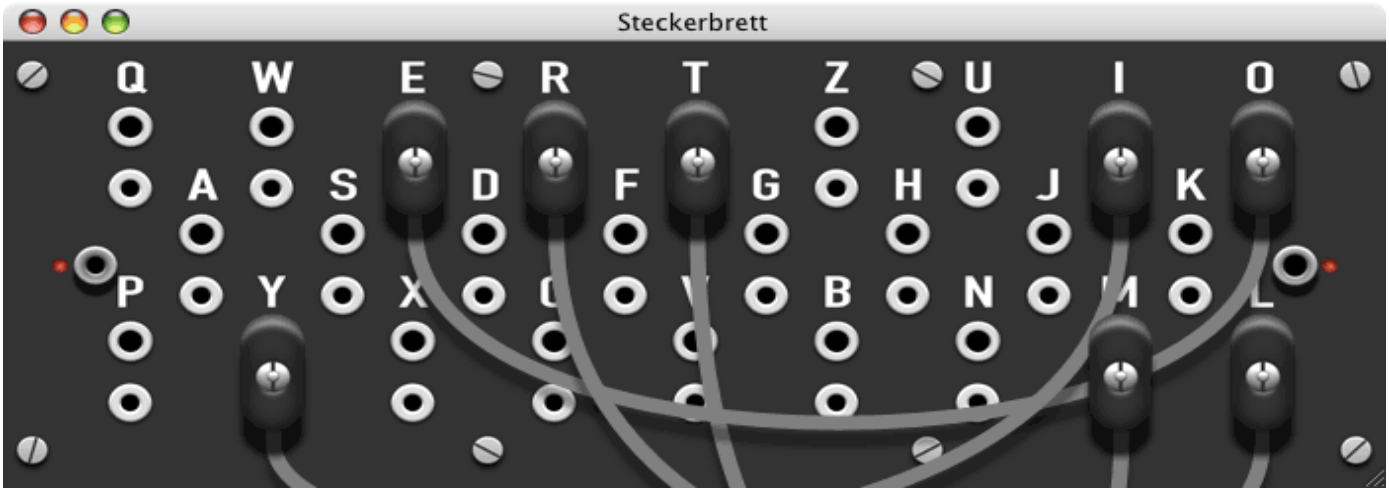
Standard Keyboard:

It's a simple keyboard.



Plug board:

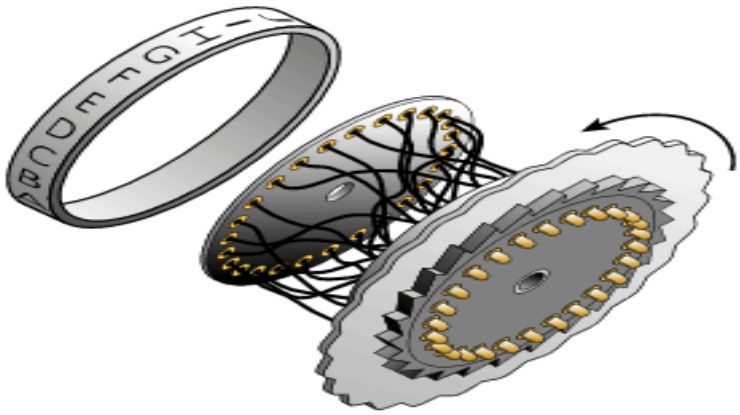
A plug board, or control panel (the term used depended on the application area), is an array of jacks, or sockets (often called hubs), into which patch cords can be inserted to complete an electrical circuit. Control panels were used to direct the operation of some unit record equipment.



https://en.wikipedia.org/wiki/Enigma_machine#Plugboard.

Reflector (lamp board):

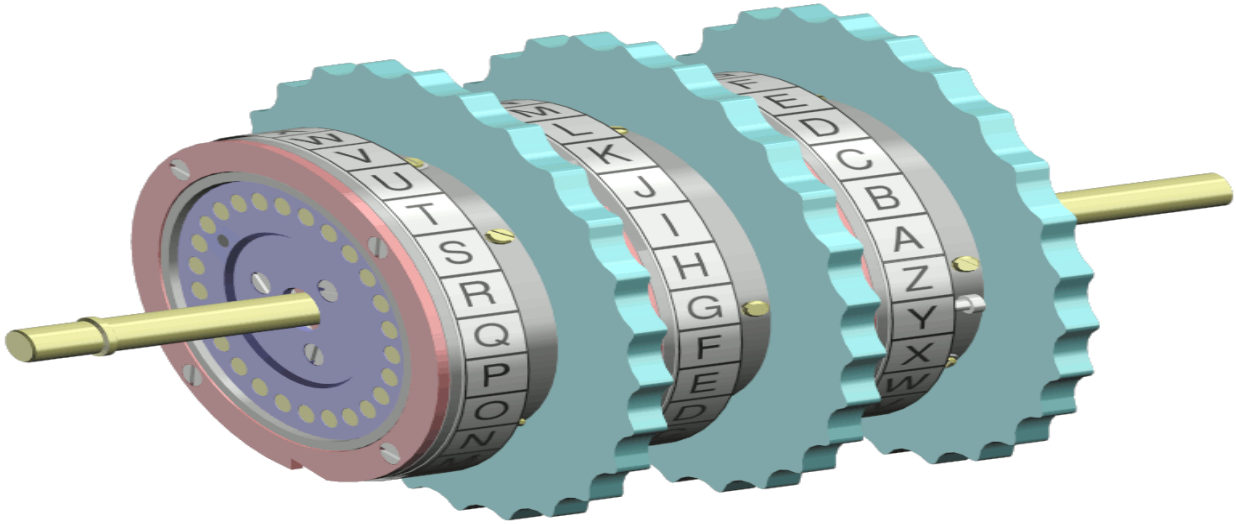
Reflector is the lightning box which reflect the keys which was pressed by the standard keyboard. Enter the first letter of your message on the keyboard and a letter lights up showing what it has replaced within the encrypted message. At the other end, the process is the same: type in the “cipher text” and the letters which light are the decoded missive.



https://en.wikipedia.org/wiki/Enigma_machine#Reflector

Rooters:

Rooters are the spinning wheels in the enigma machine which is the heart of the machine. Enigma Machine is built around three physical rotors. Each takes in a letter and outputs it as a different one. That letter passes through all three rotors, bounces off a “reflector” at the end, and passes back through all three rotors in the other direction.



https://en.wikipedia.org/wiki/Enigma_machine#Rotors

Brief description of Enigma Machine Working:

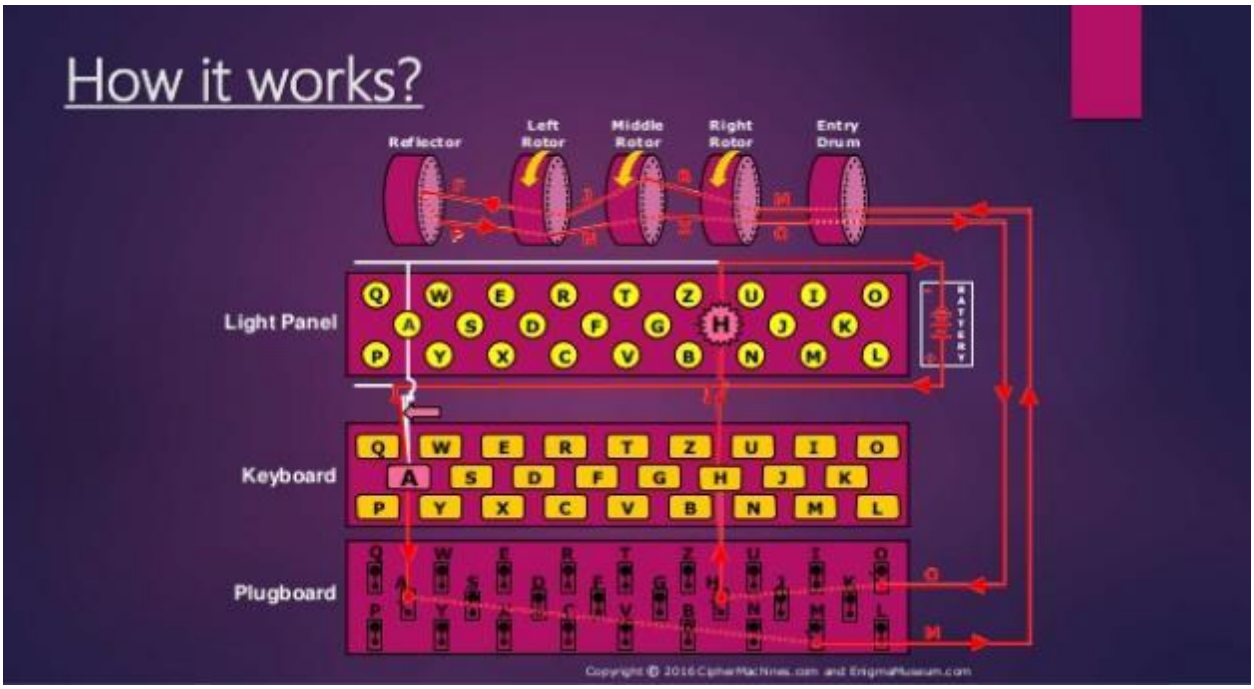
The Enigma machine was a simple cipher machine. It had several components: a plug board, a light board, a keyboard, a set of rotors, and a reflector (half rotor). The original machine looked a lot like a typewriter.

The machine has several variable settings that affect the operation of the machine. The user must select three rotors from a set of rotors to be used in the machine. A rotor contains one-to-one mappings of all the letters. Some Enigma machines had more than 3 rotors which just added to the number of possible encryption combinations. The other variable element in the machine is the plug board. The plug board allowed for pairs of letters to be remapped before the encryption process started and after it ended.

When a key is pressed, an electrical current is sent through the machine. The current first passes through the plug board, then through the three rotors, through the reflector which reverses the current, back through the three rotors, back through the plug board and then the encrypted letter is lit on the display. After the display is lit up, the rotors rotate. The rotors rotate similar to an odometer where the right most rotor must complete one revolution before the middle rotor rotated one position and so on.

As the current passes through each component in the Enigma machine, the letter gets remapped to another letter. The plug board performed the first remapping. If there is a connection between two letters, the letters are remapped to each other. For example if there is a connection between "A" and "F", "A" would get remapped to "F" and "F" would get remapped to "A". If this isn't a connection for a particular letter, the letter doesn.t get remapped. After the plug board, the letters are remapped through the rotors. Each rotor contains one-to-one mappings of letters but since the rotors rotate on each key press, the mappings of the rotors change on every key press. Once the current passes through the rotors, it goes into the reflector. The reflector is very similar to a rotor except that it doesn't rotate so the one-to-one mappings are always the same. The whole encryption process for a single letter contains a minimum of 7 remapping's (the current passes through the rotors twice) and a maximum of 9 remapping's (if the letter has a connection in the plug board).

In order to decrypt a message, the receiver must have the encrypted message, and know which rotors were used, the connections on the plug board and the initial settings of the rotors. To decrypt a message, the receiver would set up the machine identically to the way the sender initially had it and would type in the encrypted message. The output of typing in the encrypted message would be the original message. Without the knowledge of the state of the machine when the original message was typed in, it is extremely difficult to decode a message.



Also see these videos to better understand the process of enigma.

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

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

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/case-study-ww2-encryption-machines

NOTED: Main idea about all this description is that we don't use any hardware components but we simply understand the enigma machine's working to implement it on software based application. If we understand Enigma machine process so we also create its starting state (user input alphabets) and also its final state (which is encrypted output).

Language using Project (Enigma Machine):

I use java using form based interface.

X

MS FAIZA
LAB ATTENDENT