The Modified Enigma Machine
(Cryptography based project)

Dibyadarshan Hota (16CO154)
Omkar Prabhu (16CO233)

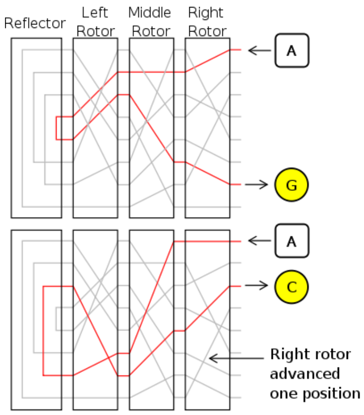
History of Enigma

Enigma machine

The Enigma machines were a series of electro-mechanical rotor cipher machines developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. 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.

Structure of Enigma

The mechanism of the Enigma consisted of a keyboard connected to a battery and a current entry plate or wheel, at the right hand end of the scrambler (usually via a plugboard in the military versions). This contained a set of 26 contacts that made electrical connection with the set of 26 spring-loaded pins on the right hand rotor. The internal wiring of the core of each rotor provided an electrical pathway from the pins on one side to different connection points on the other. The left hand side of each rotor made electrical connection with the rotor to its left. The leftmost rotor then made contact with the reflector. The reflector provided a set of thirteen paired connections to return the current back through the scrambler rotors, and eventually to the lampboard where a lamp under a letter was illuminated.



Scrambling Process

- The 3-rotor scrambler could be set in 26 × 26 × 26 = 17,576 ways, and the 4-rotor scrambler in 26 × 17,576 = 456,976 ways.
- With six leads on the plugboard, the number of ways that pairs of letters could be interchanged was 100,391,791,500 (100 billion) and with ten leads, it was 150,738,274,937,250 (151 trillion).

Cracking the Enigma code

- Marian Rejewski spotted the Germans' major procedural weakness of specifying a single indicator setting (Grundstellung) for all messages on a network for a day, and repeating the operator's chosen message key in the enciphered 6-letter indicator. That procedural mistake allowed Rejewski to decipher the message keys without knowing any of the machine's wirings.

- Alan Turing reviewed decrypted messages and determined that the word eins ("one") appeared in 90% of messages. Turing automated the crib process, creating the eins Catalogue, which assumed that eins was encoded at all positions in the plaintext. The catalogue included every possible rotor position for eins with that day's wheel order and plug board connections.

Alan Turing

Marian Rejewski

Project Idea

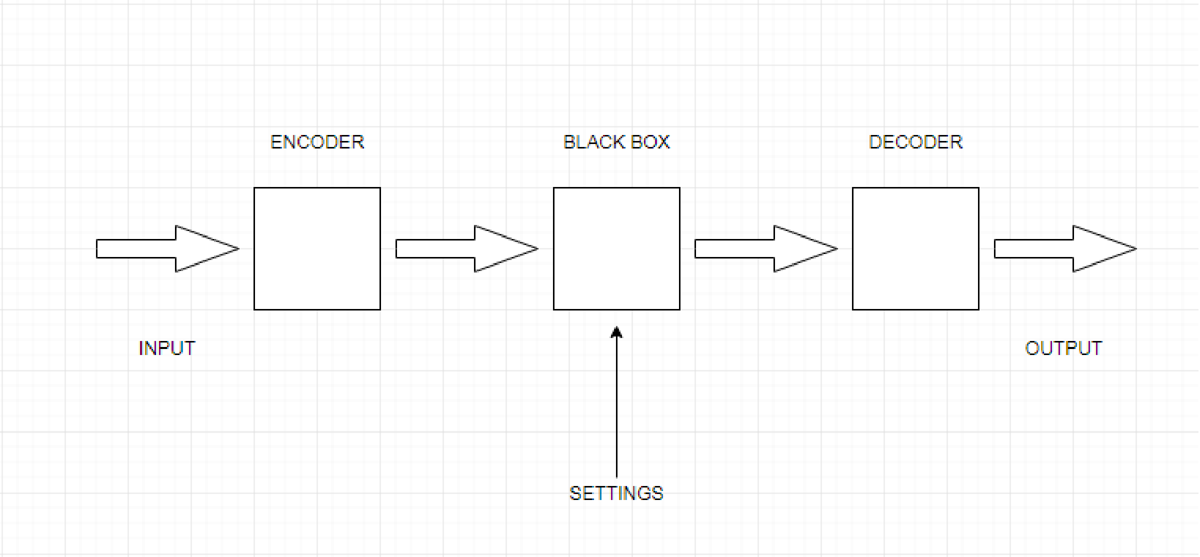
We have designed a circuit which resembles the working of the Enigma machine. It uses combinational circuits to encrypt the data entered by the user.

Encoding

The circuit makes use of multiple black boxes (instead of the rotors which were present in the original machine) in which all 26 English alphabets are mapped to another alphabet (randomly, so that it cannot be deciphered). Any one of these blocks can be selected by the person who wants to encrypt the data by choosing an arbitrary number. This number must be incremented by one before the user enters the next alphabet. This is done to ensure that *even if the same alphabet is entered multiple times the output is not repeated*.

Decoding

The encrypted data can be decoded, provided that the initial settings (the number and blocks which were chosen while encoding) are known to the person who wants to decode the information. The reflected code makes it possible to decode the encoded data.



References

- https://en.wikipedia.org/wiki/Enigma_machine
- https://www.youtube.com/watch?v=G2_Q9FoD-oQ&t=425s
- https://en.wikipedia.org/wiki/Enigma_rotor_details
- https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma