Report on Enigma

Name: Gaurav Singh

Roll No: C_70 Subject: Application Security

Course code : CCT310-3

Department: CSE(Cyber Security) Section: C

The Enigma machine is an electro-mechanical encryption device that was used extensively by the Germans during World War II to encode and decode secret messages. The Enigma machine was invented by Arthur Scherbius, a German engineer, in the early 1920s. It was designed to provide secure communications for both military and commercial purposes.

The Enigma machine uses a combination of mechanical and electrical components to encrypt messages. It consists of a keyboard, a set of rotors, a reflector, and a lamp board. The keyboard is used to input the plaintext message, which is then encrypted by the machine. The encrypted message is displayed on the lamp board.

The heart of the Enigma machine is the set of rotors. The rotors are cylindrical wheels with 26 electrical contacts on each side. Each rotor has a different wiring pattern, which is set by adjusting a series of internal wiring connections. The wiring pattern determines how the electrical signal is passed through the rotor, which changes the character that is displayed on the lamp board.

The Enigma machine uses three rotors, which can be selected from a set of five. The three rotors are arranged in a specific order, which is known as the rotor settings. The rotor settings determine the encryption key that is used to encrypt the plaintext message.

The reflector is another critical component of the Enigma machine. It is a thin metal plate with a set of electrical contacts that are wired in a specific pattern. The reflector sits between the three rotors and the lampboard. When a character is typed on the keyboard, it is sent through the rotors and then reflected by the reflector. The reflected signal is then sent back through the rotors, which changes the character that is displayed on the lampboard.

The Enigma machine uses a unique encryption key for each message that is encrypted. The encryption key is determined by the initial rotor settings, the initial rotor positions, and the plugboard settings. The plugboard is a set of cables that are used to swap pairs of letters before they are encrypted. This provides an additional level of complexity to the encryption process.

The Enigma machine was considered to be unbreakable until the Allies were able to obtain a copy of the machine and make significant progress in cracking its code. The cracking of the Enigma code was led by Alan Turing, a British mathematician and computer scientist. Turing developed a machine called the Bombe, which was used to crack the Enigma code.

The Bombe was a machine that was designed to simulate the Enigma machine and determine the rotor settings for a given encrypted message. The Bombe worked by using known plaintext to eliminate possible rotor settings until a single set was left. This process was repeated for each message that was intercepted.

In conclusion, the Enigma machine was a highly complex encryption device that was used extensively by the Germans during World War II. Its encryption key was based on the initial rotor settings, the initial rotor positions, and the plugboard settings. The Allies were eventually able to crack the Enigma code using the Bombe machine, which was designed by Alan Turing. The cracking of the Enigma code is considered to be one of the most significant achievements of World War II and is a testament to the power of cryptography and codebreaking.

Code for Enigma

```
>>> r1 = Rotor("VEADTQRWUFZNLHYPXOGKJIMCSB", 1)
>>> r2 = Rotor("WNYPVJXTOAMQIZKSRFUHGCEDBL", 2)
>>> r3 = Rotor("DJYPKQNOZLMGIHFETRVCBXSWAU", 3)
>>> reflector = Reflector("EJMZALYXVBWFCRQUONTSPIKHGD")
>>> machine = Machine([r1, r2, r3], reflector)
>>> x = machine.encipher("ATTACK AT DAWN")
>>> machine.decipher(x)
'ATTACK AT DAWN'
```