**PROJECT EXHIBITION -2**

**RESEARCH PAPER**

**PROJECT TITLE – “SOFTWARE APPROACH TO ENIGMA MACHINE”**

**ABSTRACT:-**

**The Enigma Machine**

Enigma is derived from the Latin word aenigima, which means mysterious, Cipher is from the Arabic word sifr (empty). In cryptography [5] this word is used for the algorithm that does encryption or decryption.

Enigma Cipher Machine is the name of an electro-mechanical rotor cipher machine which was first developed in Germany to provide security to commercial communication among companies and banks just after the 1st world war, around 1917. The Dutch invented these rotor based cipher machines earlier in 1915, however officially the Enigma Cipher Machine was first developed by Arthur Scherbius in 1918 and Enigma was just a brand name. Later several versions of Enigma were developed and named Enigma A, B, C, etc.

In 1926 the German Army started taking interest in Enigma machines due to its specific and high security strength. In 1927 they build their first prototype, and used it exclusively to test its capacity. The final version for use in the German army was Enigma-I and was ready for deployment by 1932. Initially the Enigma cipher machines were free for use by any organisation. But after 1932, the German army changed the rule and there after use of any Enigma machine had to be approved by the German Army. By this time many other countries were also involved in making such cipher machines.

The Enigma machine is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication.

In this project we are trying to show how the actually Enigma machine work based on Software Approachs.

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine. And also we try to write a program to decrypt the secret code produced by Enigma machine.

An Enigma machine is a electro mechanical rotor cipher machines used for the encryption and decryption of secret massages.

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine.

In this project we have operate the software processing-4 and write the separate program for each part of Enigma machine like as rotor , reflector.

In World War II, the Nazi military employed an encryption scheme that addressed the weakness of substitution ciphers. The scheme, implemented by typewriter sized devices known as Enigma machines, gave the Nazis a tactical advantage that greatly contributed to their early success in the war.

Using computers, the Allies were eventually able to break the Enigma code, giving them an intelligence edge that changed the balance of the war.

**OVERVIEW:-**

In this project, the team will create a Java program which will emulate an Enigma Machine and produce accurately encrypted or decrypted results from a given input. This software can be used as an educational device, as a historical piece, or as a tool for puzzle creation and decryption in intellectual social gatherings. The team will also spend a portion of the project researching and implementing possible algorithms for decrypting communications that have been encrypted with the Enigma Machine software. These methods may include the following:

Completed Goal – Decryption with a known or partially known cryptographic key. (Machine configuration)

Completed Goal – Brute force, statistical, or other modern techniques not available to WWII cryptographers

Stretch Goal (Researched, but not implemented) – Decryption with a “discovered” codebook (List of possible cryptographic keys)

Stretch Goal (Researched, but not implemented) – Decryption by comparison to a different message encrypted with the same key

Stretch Goal (Researched, but not implemented) – Decryption by exploiting known flaws in the machine.

**Design and User Interface**

The Enigma Machine version will determine the complexity of the project. An early machine may have three rotors and no plug board. A later version could have four rotors of a possible subset of eight to ten and a plug board. The goal of this project is to provide an Enigma Machine of variable version, allowing the user to select the number and type of rotors used and if the plug board and ring settings will be required. The user will be provided multiple options for

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine.

In this project we have operate the software processing-4 and write the separate program for each part of Enigma machine like as rotor , reflector.

In World War II, the Nazi military employed an encryption scheme that addressed the weakness of substitution ciphers. The scheme, implemented by typewriter sized devices known as Enigma machines, gave the Nazis a tactical advantage that greatly contributed to their early success in the war.

Using computers, the Allies were eventually able to break the Enigma code, giving them an intelligence edge that changed the balance of the war.





**Literature Review :-**

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there's no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.It's difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it's a good idea to choose one that's been in use for several years, and has successfully resisted all attacks.For more information, see Data encryption and decryption functions.