Evolution in Encryption and Decryption Methodologies

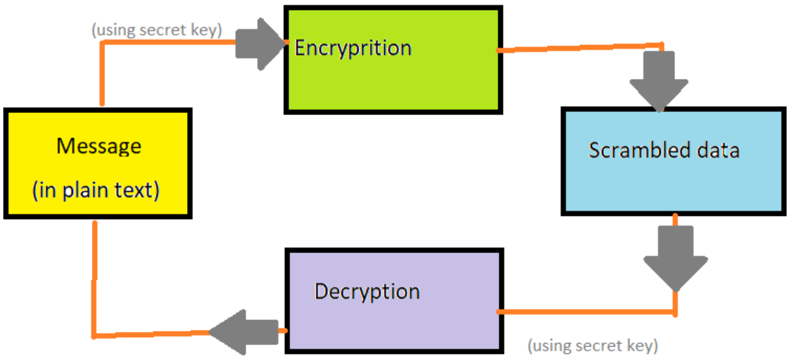
Swayam Shirsath

Nanded, India

Abstract - Nowadays, the internet is used for various purposes around the world. We can share data and information, including personal or private details that we want to keep secret, such as bank details, credit card numbers, passwords, and addresses. However, sometimes this data may be hacked or misused. Therefore, it is essential to protect it by providing security and encryption. Encryption involves scrambling or changing the text to hide the original information. Decryption is the process of reversing this action, allowing us to read the scrambled data.

Introduction - Encryption provides security and protects data transmitted across networks. The process of transforming simple text into an apparently inappropriate form, the cipher text, by using an encryption key and mathematical algorithm is called encryption. The process that reverses this transformation and reverses the effect of encryption by using a decryption key and mathematical algorithm is called decryption.

In short, encryption converts plaintext into an unreadable form, and decryption conversely transforms that unreadable text into readable form by using a decryption key. In our daily lives, products that require encryption protection, such as computer games, apps, phone calls, and video chats, all require security, which encryption provides.



History - Around 1900 BC, the scribes in Egypt used some unusual hieroglyphic symbols instead of regular ones in the chamber of the tomb of nobleman *Khnumhotep II*. The purpose was not to hide something but to make it special.

Chanakya's '*Arthashastra'* is a well-known book in Sanskrit based on economic, political science, statecraft, and military strategy. It is mentioned in that book that *Chanakya* gave duties to his agents in secret writing.

During battles, Spartans used a *scytale* device to send secret messages.

Around 100 BC, *Caesar's cipher* (named after Julius Caesar) became a very famous method used for encryption, Julius Caesar encoded his orders or commands in a secret code so that if the message fell into the wrong hands, they would be unable to read it. The cipher shifted alphabet by 3 places.

From the 15th century, combinations of multiple alphabets were used in polyalphabetic ciphers, increasing the effectiveness of encryption.

During the 16th century, *Vigenère* designed a cipher where an encryption key was used for the first time. However, this cipher could be easily broken, as Caesar cipher.

During World War 2, the *Enigma machine* was used for encryption by German soldiers. This machine was invented by *Arthur Scherbius*. The Enigma machine used an electromechanical rotor system, which was a complex encryption tool. It had an attached keyboard to scramble letters.

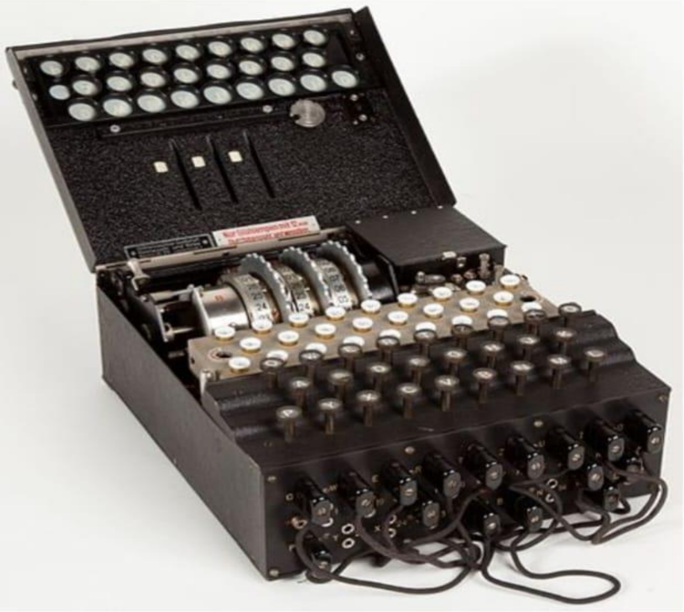


Figure 1 Enigma Machine

Modern Cryptography- In the modern world, instead of swords and shields, computers are new weapons so, computer data needs to be secure. Therefore, we need to encrypt messages so that it is very difficult to crack. Modern cryptography is based on binary bit sequences. For better encryption, computers use mathematical algorithms and equations along with a secret key, which is known as the *encryption key*. Due to these complex mathematical algorithms and the absence of a secret key, attackers are unable to get the original information. The algorithm for coding is known only to authorized individuals to provide security to cyber systems and make it difficult to break. The cybersecurity industry increases the degree of complexity and barriers to ensure data security.

Today, two types of algorithms are used: *symmetric key algorithms* and *asymmetric key algorithms*.

In symmetric key algorithms, mathematical parameters are used to encrypt and decrypt data. It has a secret key, and the same key is used for both encryption and decryption. Symmetric key algorithms are faster and more efficient than asymmetric key algorithms, but they are less secure than asymmetric key. There are several types of symmetric key algorithms, such as Block ciphers, Stream ciphers, Feistel ciphers, substitution ciphers, and permutation ciphers.

In asymmetric key algorithms, two different keys are used for encryption and decryption. This type of algorithm is also called a public key algorithm. It is used in *Blockchain technology* and *digital signatures*.

RSA algorithm, which was invented by Ron Rivest, Adi Shamir and Len Adleman in 1977, is very popular in encryption technology. It uses different keys for encryption and decryption. It uses *a public key* for encryption, and the *private key* is used for decryption, and vice versa. Both the keys are related mathematically.

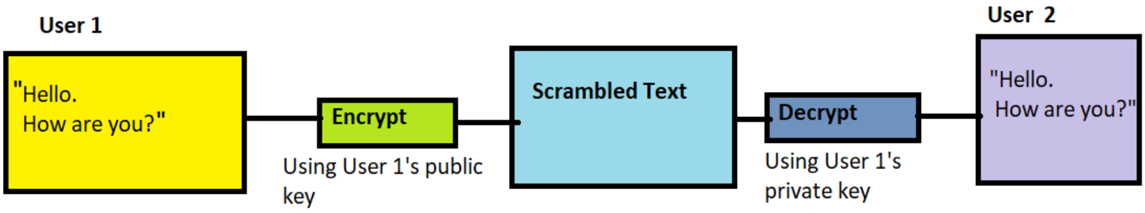


Figure 2 Encryption and Decryption using Public key and Private key

Major Encryption algorithm are: Triple DES, AES, Twofish, ARIA, IDEA, HC-128 etc.

Conclusion- From the past, encryption technology has been evolving and undergoing modifications to provide more and more security to our data and information. The growth of encryption technology has also given rise to many legal issues in the field of information technology. Cryptography has been used as a weapon by many governments for spying and treason. There are also bans and limitations on its use and export, and it may be illegal or permitted by law in some jurisdictions. Encryption is also very important in cases of copyright violation, digital rights management, and controversies surrounding digital media.

References-

1] Kessler, Gary (November 17, 2006) "An Overview of Cryptography".

2] "Caesar Cipher in Cryptography" GeeksforGeeks.

3] Hern, Alex (2014-11-14). "How do the Enigma machine works?".

4] Bellare, Mihir. "Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements." Springer Berlin Heidelberg, 2000. p. 1.

5] Kelly, Maria (December 7, 2009). "The RSA Algorithm: A Mathematical History of the Ubiquitous Cryptological Algorithm"

6] Delfs, Hans; Knebl, Helmut (2007). "Symmetric-key encryption". *Introduction to cryptography: principles and applications*.