A REVIEW PAPER ON CRYPTOGRAPHY

Mr. Mounesh K Arkachari[1], Mr. Ranjith[2], Mr. Sreejith R[3], Mr. Preetham[4] , Sanjay G K[5]

[1]*Assistant Professor, Dept. of ISE, AIET Moodbidre, Karnataka, India -574225*

[2,3,4,5]*Student, Dept. of ISE , AIET Moodbidre, , Karnataka, India -574225*

ABSTRACT

Any kind of digitally stored information is called data. Asset protection is the main goal of security. Protective digital privacy measures used to stop unwanted access to computers, private databases, and webpages are referred to as data security. Cryptography is always evolving and evergreen.

By offering features for data encryption and user authentication, cryptography safeguards its users. Reducing the amount of bits or bytes required to represent a given set of data is known as compression. It makes more data storage possible. One common method for transmitting important information covertly is through cryptography. Among the various cryptographic methods available, one of the most potent methods is AES.

Keywords:- *data security, encryption, decryption, algorithm, cipher, and cryptography.*

1. INTRODUCTION

Cryptography is a method of ensuring message confidentiality. In Greek, the phrase has a special meaning: "hidden writing." Nowadays, however, individuals and organization's privacy is protected by high-level cryptography, which ensures that information delivered is secure and only the authorized receiver has access to it [1].

Cryptography is a traditional method that is continuously being explored, with historical roots. Examples reach back to 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome. Hundreds of millions of people use cryptography on a regular basis to protect data and information, while the majority are unaware of it. Cryptographic systems, in addition to being immensely helpful, are also extremely brittle, as a single programming or specification error might compromise them.

2. LITERATURE REVIEW

A technique for achieving data and message secrecy is cryptography. According to Abdalbasit Mohammed Qadir et al. [1], it is used at a higher level these days, but no one is even aware that it is being used. It is an extremely old technique that is continuously evolving. According to Susan et al. [2] Because crackers are constantly coming up with new ways to attack computers and networks, new courses are developed to stop them from happening in the future. Security for networks and computers is a new and developing field of technology. The primary focus of these security courses is on mathematical and algorithmic ideas such as encryption and hashing algorithms. Sandeep Tayal and others. [3] talk about how the rise of social media and e-commerce websites highlights a significant information security problem: the creation of massive amounts of data and their safe transmission over networks. This is where the use of cryptography and its techniques becomes crucial. This paper discusses the various techniques used by networks to secure data transfer and encrypt data. Information security has become a challenge in the field of computers and networking, as demonstrated by Anjula Gupta et al. [4]. The various asymmetric encryption techniques used to secure and encrypt data are also covered in this essay. conducted research by N. Varol and colleagues. [5] are symmetric encryption techniques that require first converting the content to be encrypted. Regarding the objectives of cryptography, James L. Massey [6] identifies two primary objectives that cryptography seeks to accomplish: confidentiality and/or authenticity.

3. CRYPTOGRAPHY CONCEPT

A cryptographic system's fundamental idea is to encrypt data or information so that an unauthorized individual cannot decipher its meaning. Cryptography is frequently used to transmit data over insecure channels, like the internet, or to make sure that, even in the event that unauthorized individuals gain access to the data, they are unable to understand what they are seeing. In the field of cryptography, the data that has been obscured is referred to as "plaintext," and the method used to hide it is called "encryption." We refer to the encrypted plaintext as "ciphertext." This is achieved through a collection of ideas referred to as "encryption algorithms." An "encryption key," which is supplied to the encryption algorithm along with the data as input, is typically used in the encryption process. With the help of a "decryption algorithm" and related "decryption key," the information can be extracted by the receiving end.

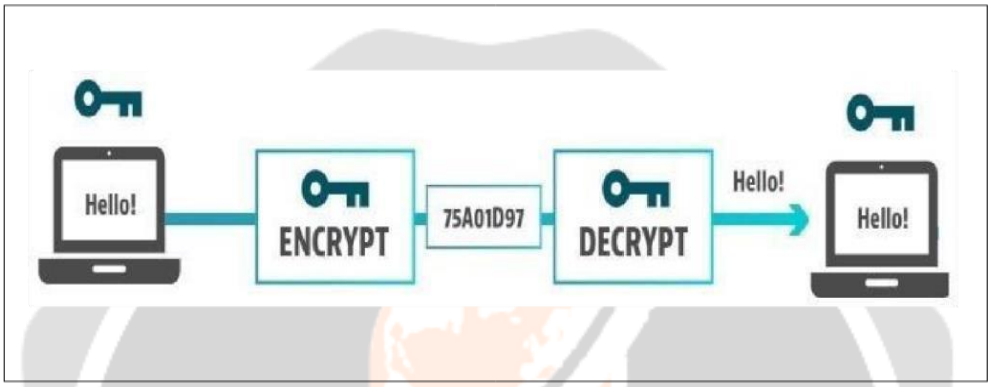

Figure 1: Cryptography concept

HISTORICAL ALGORITHMS

The history of cryptography extends back to the 1800s. The earliest cryptographic algorithms are covered in this section; they were in use long before the idea of public keys was developed.

Caesar Cipher:

This is among the first ciphers that Julius Caesar created. This was created by Rome's Julius Caesar as a weapon in battle. This was accomplished by shifting each English letter's alphabet by three positions, which produced the cipher text. All it took to break it was to move the alphabet back three positions. Even though it was very simple to break, this was a great tool in ancient warfare. A shift algorithm is now also frequently used as a Caesar Cipher. This method shifts the number by three, but it could also be anywhere from one to twenty-five.

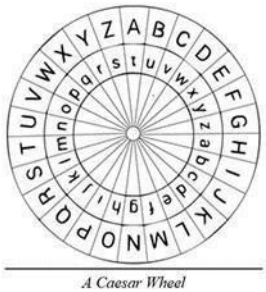

Fig. 2 Caesar Wheel

Simple Substitution Cipher

It is also referred to as the Monoalphabetic Cipher, and its name accurately describes it. Every alphabet is changed for encryption by the random letter that corresponds to it in the substitution table. Decryption operates in the exact opposite manner.

Fig 3. Substitution Cipher Table

4. TYPES OF CIPHER

There are many different types of encryption. The methods of operation and the use of one or two keys distinguish modern figures from calculations made in the past of cryptography, which are generously extraordinary to modern tactics. Techniques for encrypting data can be divided into symmetric key generation. A symmetric-key cryptography calculation is one in which the message is first scrambled and then decoded using the same cryptographic key. In fact, it is sufficient such that registering the unscrambling key from the encryption key and vice versa should be anything but challenging. Deviated key calculations are cryptographic operations that use two different but related cryptographic keys to jumble and unjumble data. Science explains the connection between the two keys: an open key is distributed to enable encryption by any sender, while a private key is kept secret by the beneficiary and enables decoding. A message that has been jumbled by a calculation using one key can be unjumbled by a similar calculation (such as RSA). Today's basic hilter-kilter encryption computations are all based on the Diffie-Hellman key agreement algorithm. There are two types of symmetric key figures: those that normally chip away at image squares and those that don't .

5. MODERN ALGORITHMS

Three primary categories have been established for the algorithms following the introduction of the "Public Key":

1) Cryptographic Hash Functions

2) Symmetric Encryption

3) Asymmetric Encryption

Symmetric Encryption

This kind only requires one key to be used for both encryption and decryption. In a symmetric exchange, the key must be exchanged by both parties in order to decrypt the message. A third party cannot decipher the encrypted message, and the recipient receives the key which reverses the algorithm and returns the ciphertext to plain text.

These also come in two varieties: stream (RC4, RC5, etc.) and block (DES, 3DES, AES, etc.).

Cryptographic Hash Functions

Another term for these is Pseudo Random Functions (PRF). It accepts a variable length string as input and, after applying a hash function, outputs a fixed length hash. The following qualities must be present in a hash function:

- It needs to be immobile.
- It must be totally impervious to collisions, meaning that two distinct inputs cannot possibly produce the same hash value.

Asymmetric Encryption

Because there is already an existing symmetric algorithm, the use of asymmetric encryption is a frequently asked question. As symmetric exchange relies on a single key for both encryption and decryption, data security would be compromised if this key were compromised by an outsider. This is where the usefulness of asymmetric encryption is shown. It employs a public key for encryption and a private key for decryption, two different keys for each function. The multi-key system turns out to be an ingenious and safe method for the two parties to exchange keys. Basically, the recipient owns both keys, which is how it operates. Using the recipient's public key, the sender encrypts the data before sending it to the recipient, who uses the private key to decrypt it. Because of its transparency, this type of cryptography is also referred to as public key cryptography. It is widely used in many networking and internet concepts, including digital signatures and the TLS/SSL handshake, to mention a few.
Asymmetric encryption is used by several algorithms, such as Diffie Hellman, DSA, RSA, and others. This section goes into great detail about the Diffie Hellman key exchange.

6. DIGITAL SIGNATURES

Digital signatures were nonexistent prior to the development of computers, in contrast to cryptography.
Since the advent of computer communications, there has been a need to talk about digital signatures, particularly in business settings where several parties are involved and each needs to promise to uphold their declarations and/or proposals. Centuries ago, people first discussed the idea of unforgeable signatures—but those were handwritten signatures. In a paper titled "New Directions in Cryptography," Diffie and Hellman first presented the concept of digital signatures. Consequently, authentication by itself is unable to bridge the trust gap between a sender and a recipient in this scenario. In addition, a digital signature that is comparable to a handwritten signature is needed.
Digital Signature Requirements:

The "digitalization" era that we are currently experiencing and living in gave rise to the relationship that established the connection between encryption and signature. An unforgeable signature schema would need to meet the following requirements:

• The option to create a signature on any chosen document should be available to every user.

• Every user should be able to quickly ascertain whether a given string is actually the signature of another user.

On documents that the original owner did not sign, no one should be able to create signatures.

Digital Signature Principles:

This ability to demonstrate that a user or individual created a message is necessary both inside and outside of the digital domain. In the modern world, this is accomplished by using handwritten signatures. When creating digital signatures, public-key cryptography is used; the general idea is that the person signing a document or message uses a

private key (referred to as the private-key), and the person receiving the message or document needs to use the corresponding public-key.

7. CONCLUSION

In order to provide more secure information transmission to all users connected worldwide, the field of cryptography is expanding in tandem with the growth of the internet. Since data integrity is always in danger, confidentiality is a crucial consideration for organizations. In addition to data security, cryptography guarantees strong, reliable, and secure network security. Consequently, creating a secure network tailored to a company's requirements aids in preventing operational environment hazards for the network. In the IT sector, cryptography is still the most effective way to protect the privacy of financial, personal, medical, and e-commerce data. A trustworthy security policy should guarantee the confidentiality and authenticity of data or information without compromising its availability or integrity.

8. REFERENCES

[1]. N. Sharma, Prabhjot, and H. Kaur, "A Review of Information Security Using Cryptography Technique," International Journal of Advanced Research in Computer Science, vol. 8, no. Special Issue, 2017, pp. 323-326.

[2]. Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.
[2] B. Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, London: Springer, 2010.

[3]. lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC, 2008. [3] J. Katz and Y. Lindell, lntroduct:ion t:o Modern Cryptography, London: Taylor & Francis Group, LLC, 2008.
[4]. "Network Security: Focus on Security, Skills, and Stability," 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007. S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.

[5]. "Communications cryptography," by O. O. Khalifa, M. R. Islam, S. Khan, and M. S. Shebani, in RF and Microwave Conference, 2004. Proceedings of RFM 2004, Selangor.

[6]. "Review and Analysis of Cryptography Techniques," by N. Jirwan, A. Singh, and S. Vijay

[7]. B. Schneier, "The Non-Security of Secrecy," Communications of the ACM, vol. 47, no. 10 (October 2004), pp. 120-120.