e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-2 (April 2023)
https://doi.org/10.31033/ijemr.13.2.15

A Study on Cryptography

Shaffali Wadhawan[1] and Shilpa[2]
[1]Assistant Professor, Global Group of Institutes, Amritsar, Punjab, INDIA
[2]MCA Student, Global Group of Institutes, Amritsar, Punjab, INDIA

[1]Corresponding Author: wshaffali@gmail.com

Received: 11-03-2023 **Revised:** 28-03-2023 **Accepted:** 17-04-2023

ABSTRACT

The goal of the paper is to present a general understanding of network security and cryptography. The study and application of methods to protect communication in the presence of hostile conduct. On the other hand, using both software and hardware technologies, network security refers to a collection of regulations and configurations and data. Data that is kept in our systems as well as network and data transfer through wireless networks are protected using cryptography and network security. Through the use of codes (encryption), techniques like fusing words with images, and other methods to hide information, cryptography is a network security tool used to safeguard company data and communication from cyber attacks. The study and application of methods to protect communication against malicious behaviour is known as cryptography. On the other hand, using both software and hardware technologies, network security refers to a collection of regulations and configurations intended to safeguard the accessibility, integrity, and confidentiality of computer networks and data. Data that is kept in our systems as well as network and data transfer through wireless networks are protected using cryptography and network security[4].

***Keywords*--** Cryptography, Symmetric Key, Asymmetric Key, Cyber Attack

I. INTRODUCTION

The study of secure communication methods, such as encryption, that only the message's sender and intended recipient can access, is known as cryptography. The word is derived from Krypto’s, a concealed word in Greek. It is closely related to encryption, which is the process of converting plain text into ciphertext before sending it and then back again after receiving it. The obscuring of information in photographs using methods like microdots or merging is also covered by cryptography. These techniques were employed by the ancient Egyptians in their intricate hieroglyphs, and Julius Caesar, the Roman Emperor, is credited with creating one of the earliest modern cyphers.

A method to ensure message confidentiality is cryptography. Greek gives the phrase a special meaning: "secret writing." However, in modern times, personal privacy and High-level cryptography is used by organisations to ensure that information supplied is secure and that only the intended recipient can access it . Cryptography is an ancient technology with historical roots that is continually being improved. Examples date as far back as 2000 B.C., when the ancient Egyptians used "secret" hieroglyphics. Other examples include obscure texts from ancient Greece and the renowned Caesar cypher from ancient Rome.[1]

II. ENCRYPTION

Information is turned to ciphertext during the encryption process, a type of data protection. The original plaintext data cannot be accessed without the key, which is only accessible to authorised individuals.

Even more simply put, encryption is the process of making data unintelligible to unauthorised parties. This aims to deter thieves who may have accessed a company network using pretty sophisticated methods only to discover that the data is unreadable and so useless[5].

III. SYMMETRIC KEY

Groupings in Cryptography Symmetric key cryptography is a type of encryption in which a single, shared key is used to both encrypt and decrypt a message by both the sender and the recipient. The Data Encryption Standards (DES) is the most widely used symmetric key system. (DES). When personally identifiable information needs to be encrypted, financial apps frequently use symmetric key cryptography. Symmetry cryptography increases these payment gateways' overall security index and aids in the detection of bank fraud. They are useful for securing data that is stored on servers and in data centers, which house vast amounts of information that must be encrypted with a quick algorithm to ensure little to no delay when the information needs to be retrieved by the appropriate service. To visit safe https websites while online and have all-around protection, we require symmetric encryption. It is important for ensuring the highest level of security by authenticating the website, exchanging the required encryption keys, and forming a session utilising those keys. This assists in avoiding the somewhat unsafe https website structure.

Information is encrypted and decrypted with a single key in symmetry key cryptography. Both the sender and the receiver must have access to the key, which must be kept secret. The key size being utilised determines how strong the encryption [9].

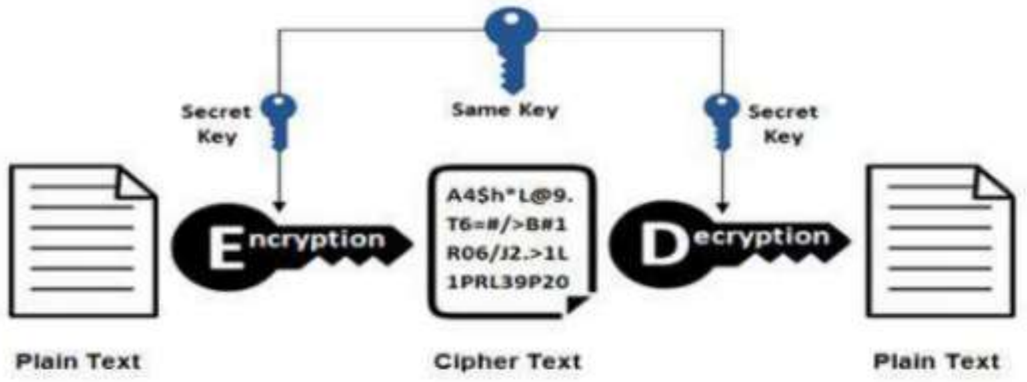

Figure 1: Symmetric Key

IV. ASYMMETRIC KEY

Asymmetric Encryption employs the use of two unique keys. Information is encrypted using a private key, and it is decrypted using a public key. Asymmetric encryption has two layers of security. A private key and a public key are the two keys that are utilised in this situation. Prior to transmission, the data is encrypted using a public key, and it is decrypted afterwards using a private key. The message's recipient must be the rightful owner of this set of keys. As seen in the graphic below, where two keys are active in the system, the public key can be distributed without limitation via messaging, blogs, and key servers. The cypher text is then transferred to the receiver without the use of any additional keys after the sender first encrypts the plain text using the receiver's private key. The receiver uses his or her private key to decrypt the ciphertext after receiving it in order to recover the plaintext. Key exchange has not been necessary at any point during the procedure. so resolving the symmetric key cryptography's most obvious problem.[13]

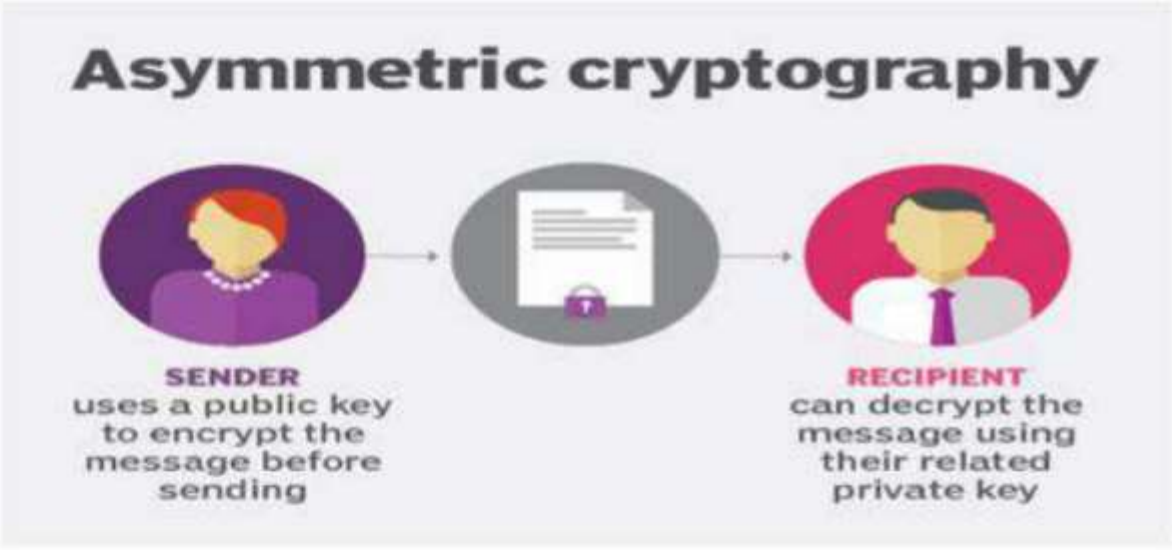
Asymmetric cryptography
SENDER
uses a public key to encrypt the message before sending
RECIPIENT
can decrypt the message using their related private key

Figure 2: Asymmetric Key

V. DECRYPTIONS

Decryption is the process of removing a coding to reveal easily understood information. The western Allies utilised decryption during World War II to decipher German military strategy concealed in covert messages.

Although spies have used decryption to decipher coded signals for decades, the majority of decryption now takes place on computers. Nowadays, practically all data is safeguarded by encryption, concealment, or conversion to a code. Your information is encrypted to safeguard your privacy whether you send an email or input a credit card number to make an online purchase. Your card can be processed and your email can be viewed by the receiver thanks to decryption [11].

VI. PRIVATE KEY

In cryptography, a private key, also referred to as a secret key, is a variable that works with an algorithm to encrypt and decrypt data. Only those parties with permission to decode the data should have access to secret keys. In both symmetric and asymmetric cryptography, private keys are crucial [15].

VII. PUBLIC KEY

A public key contains two keys. For encryption and decryption, separate keys are employed. The plain text is encrypted using a public key to create cypher text, and the recipient decrypts the cypher text with a private key to read the message [10].

VIII. RSA ALGORITHM IN CRYPTOGRAPHY

Asymmetric cryptography uses the RSA algorithm. Asymmetric really means that it utilises both the public and private keys, which are two separate keys. As implied by the name, the private key is kept secret while the public key is distributed to everyone.

Asymmetric Cryptography Illustration

1. When requesting data from the server, a client (for instance, a browser) transmits the server its public key.
2. Using the client's public key, the server encrypts the data before sending it.
3. This data is delivered to the client, who decrypts it.
Since the encryption is asymmetric, even if a third party obtains the browser's public key [12].

IX. CRYPTOGRAPHY PROCESS

Plain text - The communications to be encoded are referred to as plain content or clear content in the cryptography process.
Encryption -The process of providing cypher material is known as encryption.
Cipher text - Cipher text is the name given to the encoded communication.
Decoding - Decoding refers to the process of obtaining the plain material from the cypher content.[2]

An example of cryptography

- Consider the message “FAT RAT”
- A message is converted into a numeric form according to some scheme. The easiest scheme is to let space=0, A = 1 , B=2,... Y = 25 and Z = 26 For example, the message "FAT RAT" would become 6, 1, 20, 0, 18, 1, 20.

$$A = \begin{bmatrix} 6 & 1 \\ 20 & 0 \\ 18 & 1 \\ 20 & 0 \end{bmatrix}$$

This data was placed into matrix form. The size of the matrix depends on the size of the encryption key. Let's say that our encryption matrix (encoding matrix) is a 2 * 2 matrix. Since I have seven pieces of data, I would place that into a 4 * 2 matrix and fill the last spot with a space to make the matrix complete. Let's call the original, unencrypted data matrix A

The term "encoding matrix" or "encryption matrix" refers to an invertible matrix.

It'll be known as matrix B. This matrix must be square in order to be invertible.

Depending on the person encrypting the matrix, this may be anything. Use this matrix, please.

$$B = \begin{bmatrix} 4 & -2 \\ -1 & 3 \end{bmatrix}$$

Then, we multiply the raw data by our encoding matrix. This multiplication yields a matrix that contains the encrypted data. It'll be known as matrix X.

$$AB = \begin{pmatrix} 23 & -9 \\ 80 & -40 \\ 71 & -33 \\ 80 & -40 \end{pmatrix}$$

- The stream of numbers is the message you would convey to the other person 23,-9, 80,-40,71,-33,80,-40.

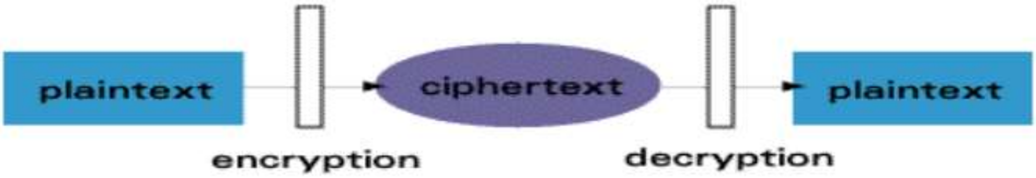

Figure 3: Basic Encryption and Decryption

X. SERVICE FOR SECURITY

The figure 3 contains following categories apply to security services:

Confidentiality

Only authorised individuals (the recipient) can read the supplied information, which is referred to as confidentiality. An unauthorised person cannot access the data being sent over the network.

Integrity

Integrity is the guarantee that digital data is accurate and can only be viewed or changed by those with the proper authorization. Included in modification are writing, status changes, and Messages can be created, deleted, delayed, or replayed.

Authentication

Verifying a person's or a device's identity is the process of authentication. The security system receives a user identity from the identification step. A user ID is used to provide this identity. Entering a login and password to access a website is a typical illustration.

Non-Repudiation

The guarantee of non-repudiation states that the holder of a signature key pair that was able to produce an existing signature corresponding to a given piece of data cannot persuade fully refute having signed the piece of data.

Control of Access

Users are identified by access control by authenticating their login information, which can include usernames and passwords, PINs, biometric scans, and security tokens.

Availability

System, application, and data availability ensures that users have access to them when they need it [8].

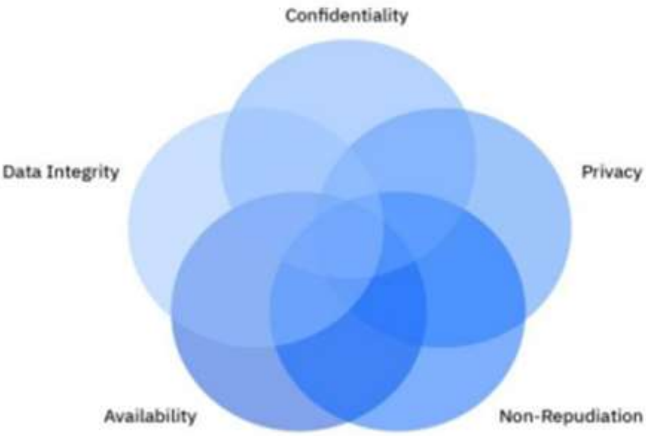

Figure 4: Categories of Service of security

XI. CONCLUSION

Since everything in today's world is online, security is crucial. The previous methods are simple to counter. Consequently, cryptography is crucial to protecting our data from being stolen or misused. Users not authorised. Only the sender and the recipient should have access to the key. Clients can employ cryptography to encrypt information and certify the identity of distinct clients. To provide secure communication, some cryptographic techniques are employed in network security. Data communication via the internet uses network security and cryptography to ensure security. Cryptography helps ensure secrecy, integrity, availability, and non-repudiation, which are the main goals of security technology. The establishment of a safe channel and link for the transmission of data and information between two entities is made possible by cryptographic methods. In the area of IT, cryptography is a constantly developing field. Data security, and by extension encryption, have grown more crucial than ever as the world becomes more technologically centred and everything is digitized[6].

REFERENCES

[1] https://www.cgmoneta.com/cybersecurity#:~:text=Network%20Security%20is%20the%20protection,or%20from%20a%20private%20networ.

[2] https://www.irjet.net/archives/V7/i4/IRJET-V7I4585.pdf.

[3] https://www.geeksforgeeks.org/the-cia-triadincryptography/#:~:text=Confidentiality%20means%20that%20only%20authorized,be%20accessed%20by%20unauthorized%20individuals.

[4] https://en.wikipedia.org/wiki/Passive_attack#:~:text=For%20a%20release%20of%20message,contents%20of%20the%20transmitted%20data.&text=When%20the%20messages%20are%20exchanged,party%20may%20capture%20the%20messages.

[5] https://en.wikipedia.org/wiki/Traffic_analysis#:~:text=Traffic%20analysis%20is%20the%20process,when%20the%20messages%20are%20encrypted.&text=Advanced%20traffic%20analysis%20techniques%20may%20include%20various%20forms%20of%20social%20network%20analysis.

[6] Krishnamoorthy, Dr & S. Chidambaranathan. *Clever cardnovel authentication protocol (NAUP) in multi-computing internet of things environment*.

[7] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). *A review paper on cryptography*. DOI: 10.1109/ISDFS.2019.8757514.

[8] S. J. Lincke & A. Hollan. (2007). Network security: Focus on security, skills, and stability. In: *37th ASEE/IEEE Frontiers in Education Conference, Milwaukee*.

[9] S. Tayal, N. Gupta, P. Gupta, D. Goyal & M. Goyal. (2017). A review paper on network security and cryptography. *Advances in Computational Sciences and Technology, 10*(5), 763-770.

[10] A. Gupta & N. K. Walia. (2014). Cryptography algorithms: A review. *International Journal of Engineering Development and Research, 2*(2), 1667-1672.

[11] N. Varol, F. Aydoğan & A. Varol. (2017). Cyber attacks targetting android cellphones. In: *5th International Symposium on Digital Forensics and Security (ISDFS 2017), Tirgu Mures*.

[12] J. L. Massey. (2986). Cryptography - A selective survey. *Digital Communications, 85*, 3-25.

[13] https://www.boxentriq.com/img/caesar-wheel.png.

[14] https://i.ytimg.com/vi/Dz1RW_W2zGI/maxresdefault.jpg.

[15] https://ehindistudy.com/wp-content/uploads/2015/10/wpid-au265a.gif.