e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

# RESEARCH ON CRYPTOGRAPHY AND NETWORK SECURITY

**M. Divya**[*1]

[*1]Dept. Of Computer Science, Fatima College (Autonomous), Affiliated, Madurai Kamaraj University Madurai, Tamilnadu, India.

DOI : https://www.doi.org/10.56726/IRJMETS33258

## 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 from malicious conduct 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 and transmitted over wireless networks are protected using network security and cryptography. Through the use of codes (encryption) and other methods to conceal information, cryptography is a network security measure that is used to safeguard company information and communication from cyber attacks.

## I. INTRODUCTION

We all rely on the internet during this era for all of our requirements, including communication, information sharing, online shopping, net banking, work, and the storage of personal information, thus we utilise the technique known as cryptography to protect the data we communicate across a network. Network security is the defence of a computer network's access to files and directories against hacking, abuse, and illegal system changes. [ 1] The resources that are stored are insured by network security. An anti-virus programme is a prime illustration of network security. Hardware, software, and cloud services are the three parts of network security.

## II. CRYPTOGRAPHY PROCESS

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

An example of cryptography

- Consider the message “RED RUM”
- 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 "Red Rum" would become 18, 5, 4, 0, 18, 21, 13.
- This information was organised into a matrix. The matrix's size is determined by the encryption key's size. Let's assume that our encoding (cryptography) matrix is a 2 by 2 matrix. I would put the seven bits of data I have into a 4 * 2 matrix and then add a space to the final position to finish the matrix. The original, unencrypted data matrix will be denoted as A.

$$A = \begin{bmatrix} 18 & 5 \\ 4 & 0 \\ 18 & 21 \\ 13 & 0 \end{bmatrix}$$

**Figure 1**

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

- There is an invertible matrix which is called the encryption matrix or the encoding matrix.We'll call it matrix B. Since this matrix needs to be invertible, it must be square.
- This could be anything; it's up to the person encrypting the matrix. I'll use this matrix.

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

**Figure 2**

- The unencrypted data is then multiplied by our encoding matrix. The result of thismultiplication is the matrix containing the encrypted data. We'll call it matrix X

$$X = A\,B = \begin{bmatrix} 67 & -21 \\ 16 & -8 \\ 51 & 27 \\ 52 & -26 \end{bmatrix}$$

**Figure 3**

- The message that you would pass on to the other person is the stream of numbers 67, -21, 16. -8, 51, 27, 52, -26.

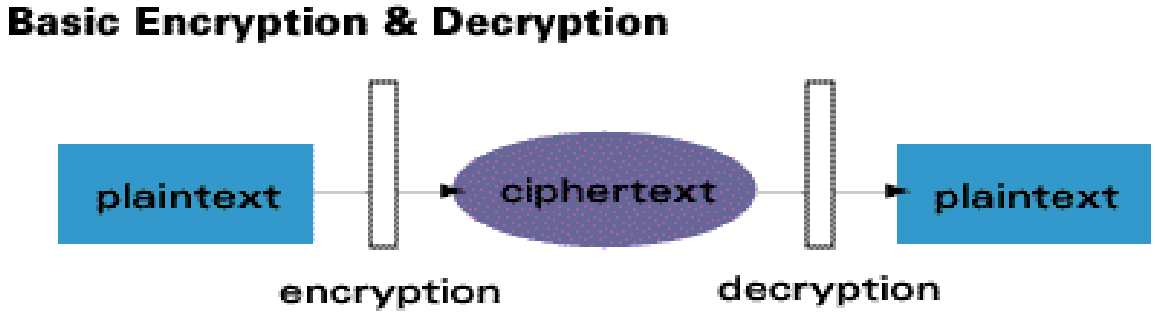


**Figure 4**

➢ The classification of security services are as follows:

**2.1. Confidentiality**

Confidentiality means that only the intended recipient has permission to examine the sent data. Unauthorized people cannot access the data being sent over the network.

**2.2. Integrity**

Integrity is the guarantee that digital data is accurate and can only be viewed or changed by those with the proper authorization. Writing, modifying status, deleting, generating, and delaying or replaying transmitted messages are all examples of modification.

**2.3. 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.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

**2.4. 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 persuadefully refute having signed the piece of data.

**2.5. Access Control**

By validating various login credentials, such as usernames and passwords, PINs, biometric scans, and security tokens, access control identifies users.

**2.6. Availability**

Availability guarantees that systems, applications, and data are available to users whenthey need them

## III. ATTACKS

**SECURITY ATTACK**

1) Interruption- Interruption is an attack on availability.

Eg- cutting of a communicationline.

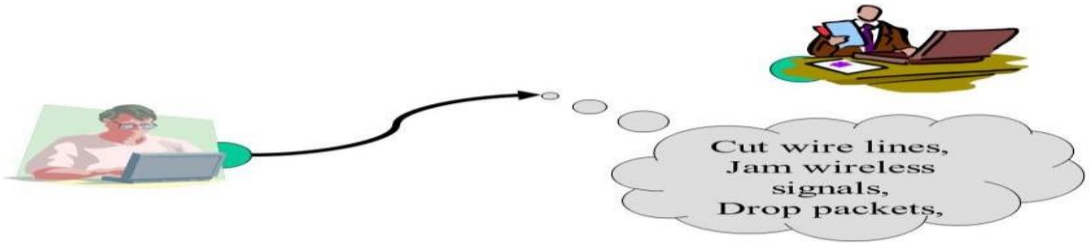


**Figure 5**

2) Interception- Interception is an attack by an unauthorized person.

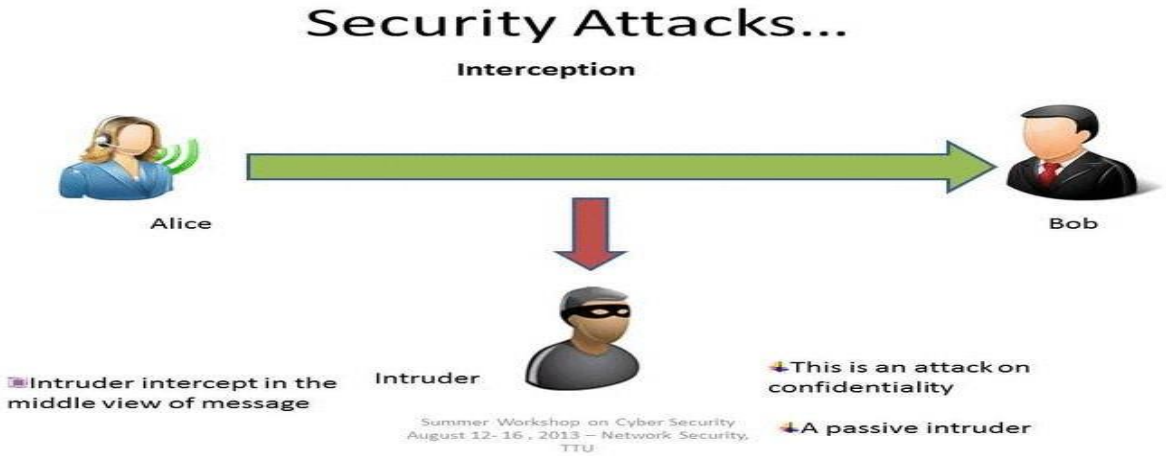


**Figure 6**

3) Fabrication- Fabrication is the attack that an unauthorized person sends to the receiver without the knowledge of the sender


**Figure 7**

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

**CRYPTOGRAPHIC ATTACKS**

1) Active Attacks

a) Masquerade- An unauthorized entity gains the access to the system.

b) Replay- Attack in which valid data transmission is maliciously or fraudulently repeated or delayed to produce an unauthorized effect.

c) Modification of messages- Attack in which part of the message is modified or message is recorded, to produce an unauthorized effect.

d) Denial of service- A Denial-of-Service attack (DoS attack) is an attack where an attacker attempts to disrupt the services provided by a host, by not allowing its intended users to access the host from the Internet.

2) Passive Attacks

a) Release of Message Content - A telephone call, an email, or a file transfer may contain private information that should not be made public. Neither the sender nor the receiver is aware that the messages could be intercepted when they are exchanged. Data encryption can stop this from happening.

b) Traffic Analysis - Traffic analysis, which can be done even when the messages are encrypted, is the process of intercepting and studying messages to determine information from communication patterns.

## IV. TYPES OF CRYPTOGRAPHY

**A. Symmetric Key Cryptography:** The practise of symmetric encryption is not new. The secret key used to encrypt and decrypt all of the communications should be known by both the sender and the recipient. Symmetric Key Systems are quicker and easier, but the sender and receiver must safely exchange keys, which is a concern.

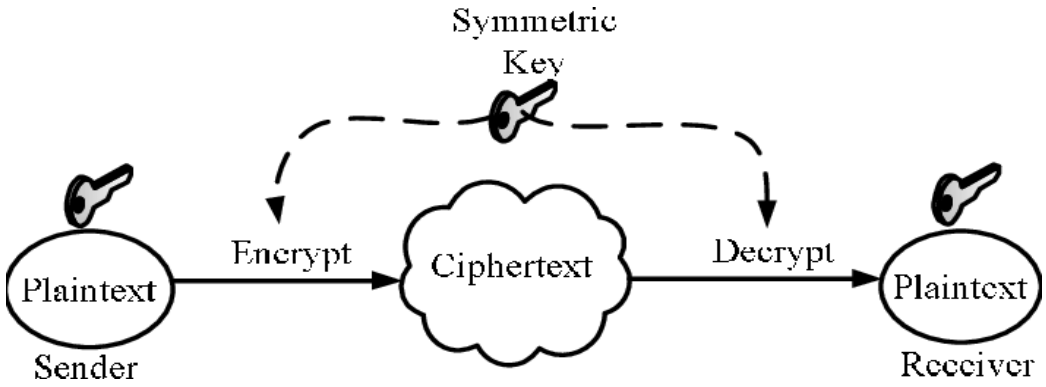


**Figure 8**

**B. Hash Function:** A hash function is a mathematical operation that yields a fixed-sized output after compressing a numerical input value into another numerical value.

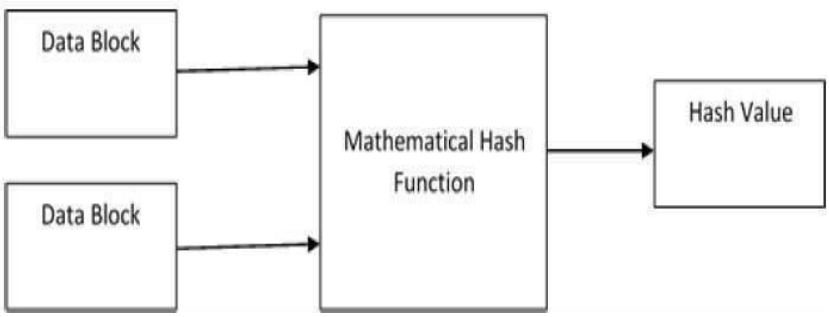


**Figure 9**

## V. APPLICATION OF CRYPTOGRAPHY

**1)** Digital Currency

**2)** E-commerce

**3)** Military purposes

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
( Peer-Reviewed, Open Access, Fully Refereed International Journal )
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com


**Figure 10**

## VI. APPLICATION OF NETWORK SERVICES

**1)** In-Flight
**2)** Emergency Response Team
**3)** App Wall
**4)** Banking
**5)** Cloud Malware Production Service
**6)** Shopping

## VII. CONCLUSION

Since everything in today's world is online, security is crucial. The previous methods are simple to counter. Consequently, to protect the data In order to protect our data from unwanted users, cryptography is crucial. 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. In order to enable secured communication, some cryptographic techniques are utilised in network security. [6] In order to offer security for data communication via the internet, cryptography and network security are used.

## VIII. REFERENCES

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

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

[3] https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/#:~: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

[5] %20exchanged,party%20may%20capture%20the%20messages.

[6] 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.

[7] Krishnamoorthy, Dr, and S. Chidambaranathan. "Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs." (2017).