Research Paper on Crytography and Network Security

Janani Ramesh

February 8, 2022

RESEARCH PAPER ON
CRYTOGRAPHY AND NETWORK SECURITY

R JANANI

Department of Artificial Intelligence & Data Science, Easwari Engineering College, Chennai, India

ABSTRACT

The paper aims to provide a broad idea about Cryptography and Network Security. Cryptography is the practice and study of techniques to secure communication in the presence of adversarial behavior. On the other hand, Network security is the set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies. Cryptography and network security are used to protect network and data communication take place over wireless networks and data which is stored in our systems. Cryptography is a network security tactic that is used to protect enterprise information and communication from cyber threats through the use of codes(encryption) using techniques such as merging words with images, and other ways to hide information in storage or transit. In this paper, we discussed about cryptography process, security mechanism, security services, attacks, types of cryptography, Steganography.

KEYWORDS-Cryptography, Network security, Encryption, Decryption

INTRODUCTION

During this pandemic, we all rely upon online for all our needs such as communication, sharing information, online shopping, net banking, work, storing personal information, etc… so we use the method called cryptography to secure the information that we share using a network. Network security is the protection of the access to files and directories in a computer network against hacking, misuse, and unauthorized changes to the system.[1] Network security acts as insurance for the stored resources. An example of network security is **an anti-virus system**. There are three components of network security: **hardware, software, and cloud services**.

The most common network vulnerabilities:

- Improperly installed hardware or software
- Operating systems or firmware that has not been updated
- Misused hardware or software
- Poor or a complete lack of physical security
- Insecure passwords
- Design flaws in a device’s operating system or the network

While a vulnerability does not guarantee that a hacker, can easily gain access to our network information. Cryptography is the branch of network security. Cryptography is origin from the

Greek word Kryptos meaning hidden, Cryptography is an application of mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and protect confidential transactions such as credit card and debit card transactions.

CRYPTOGRAPHY PROCESS

- Plain text - The messages to be encoded is known as plain content or clear content.
- Encryption - The way toward delivering cipher content is called encryption.
- Cipher text - The encoded message is called cipher content.
- Decryption -The procedure of recovering the plain content from the cipher content is called decoding[2]

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 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

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

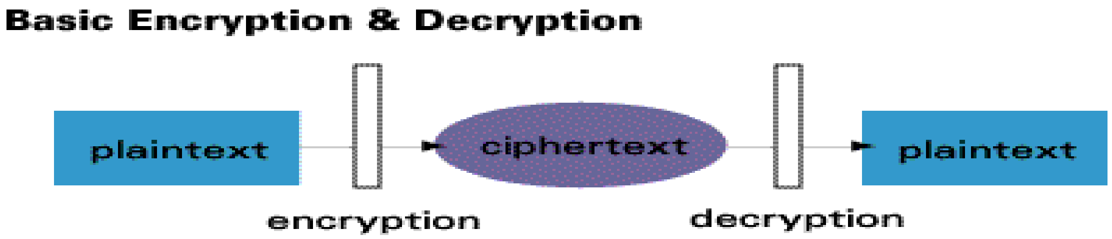
- There is an invertible matrix which is called the encryption matrix or the encoding matrix. We'll call it matrix B. Since this matrix needs to be invertible, it must be square.
- This could be anything; it’s up to the person encrypting the matrix. I'll use this matrix.

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

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

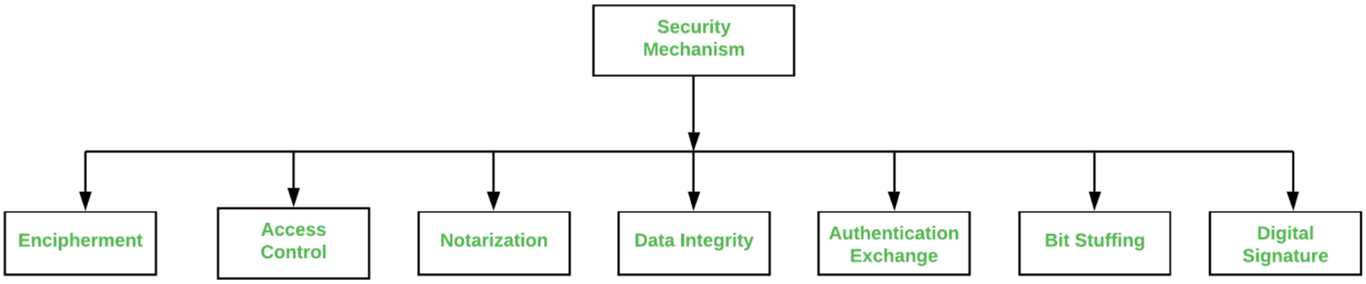
$$X = A\,B = \begin{bmatrix} 67 & -21 \\ 16 & -8 \\ 51 & 27 \\ 52 & -26 \end{bmatrix}$$

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



SECURITY MECHANISMS

- Encipherment
- Access Control
- Notarization
- Data Integrity
- Authentication exchange
- Bit stuffing
- Digital Signature



SECURITY SERVICES

The classification of security services are as follows**:**

Confidentiality

Confidentiality means that only authorized individuals(the receiver) can view the sent information. The data being sent over the network can not be accessed by unauthorized individuals**.**

Integrity

Integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so. Modification includes writing, changing status, deleting, creating, and delaying or replaying transmitted messages**.**

Authentication

Authentication is the process of verifying the identity of a person or device. Identification phase provides a user identity to the security system. This identity is provided in the form of a user ID. A common example is entering a username and password when you log in to a website**.**

Non repudiation

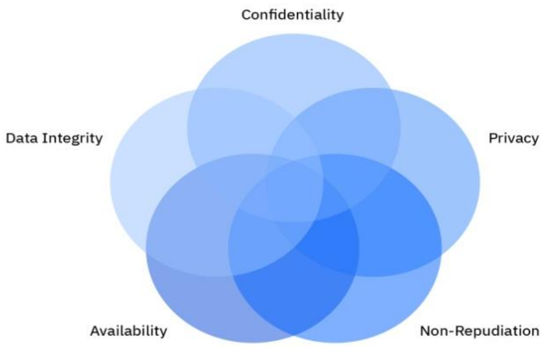
Non-repudiation refers to the assurance that the owner of a signature key pair that was capable of generating an existing signature corresponding to certain data cannot convincingly deny having signed the data**.**

Access control

Access control identifies users by verifying various login credentials, which can include usernames and passwords, PINs, biometric scans, and security tokens**.**

Availability

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

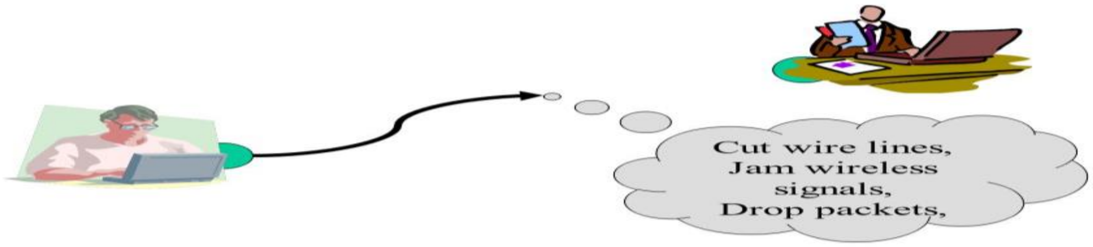


.

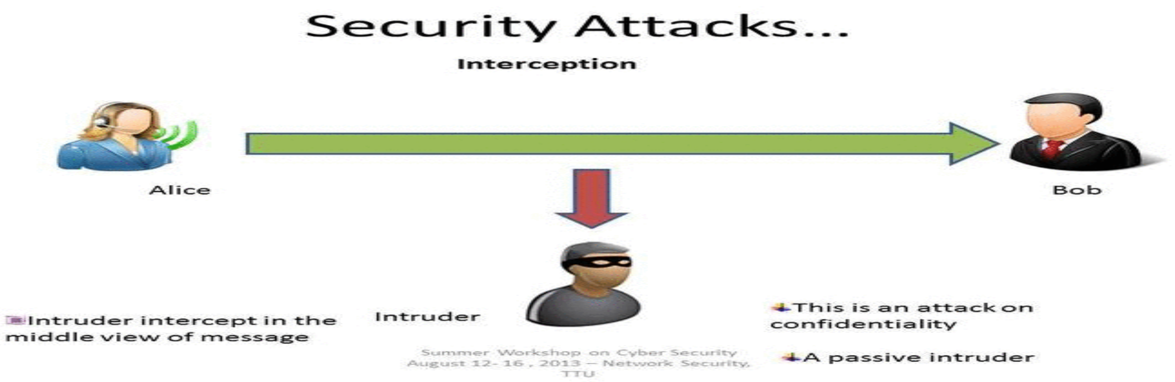
ATTACKS

I.*SECURITY ATTACKS*

1. Interruption- Interruption is an attack on availability. Eg- cutting of a communication line.



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

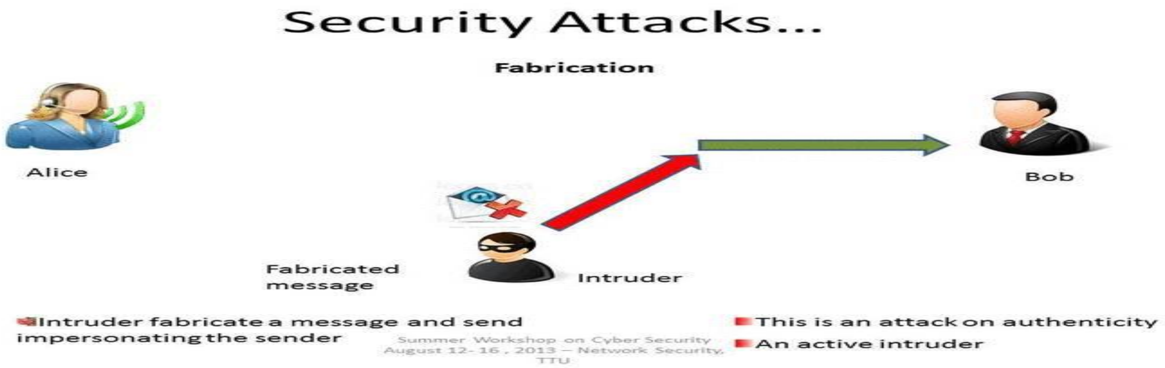

Security Attacks...

Interception

- Intruder intercept in the middle view of message
- This is an attack on confidentiality
- A passive intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

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


Security Attacks...

Fabrication

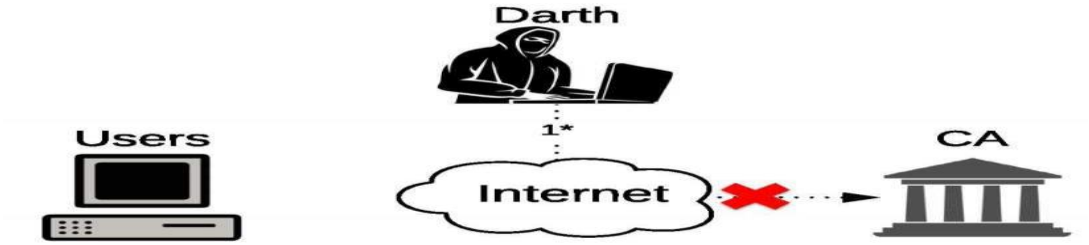
- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

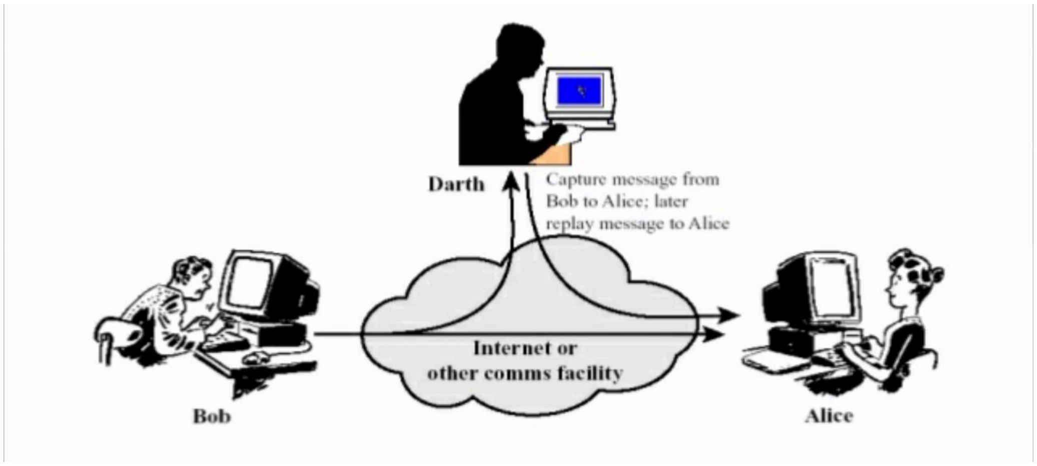
II.*CRYPTOGRAPHIC ATTACKS*

1. ACTIVE ATTACKS

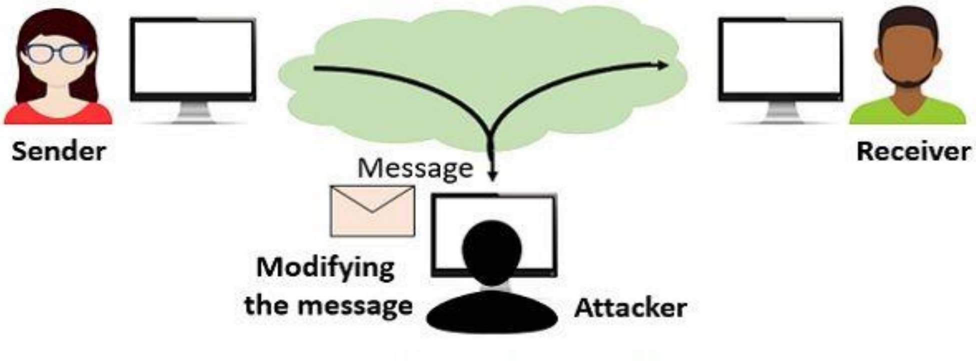
a) **Masquerade**- An unauthorized entity gains the access to the system.



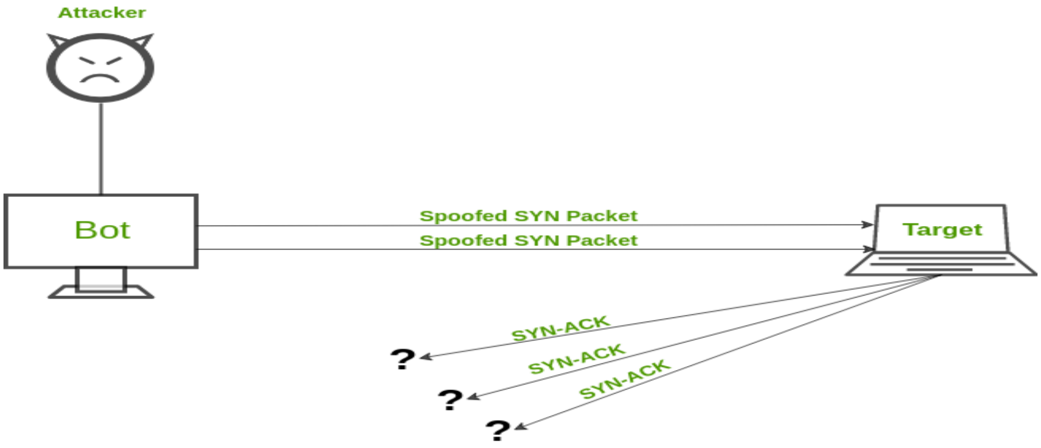
b) **Replay-** Attack in which valid data transmission is maliciously or fraudulently repeated or delayed to produce an unauthorized effect.



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

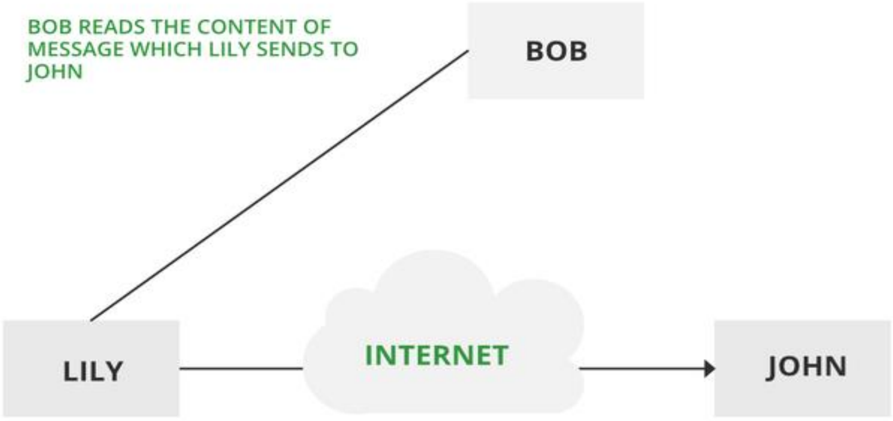


d) **Denial of service-** A Denial-of-Service attack (DoS attack) is an attack where an attacker attempts to disrupt the services provided by a host, by not allowing its intended users to access the host from the Internet.

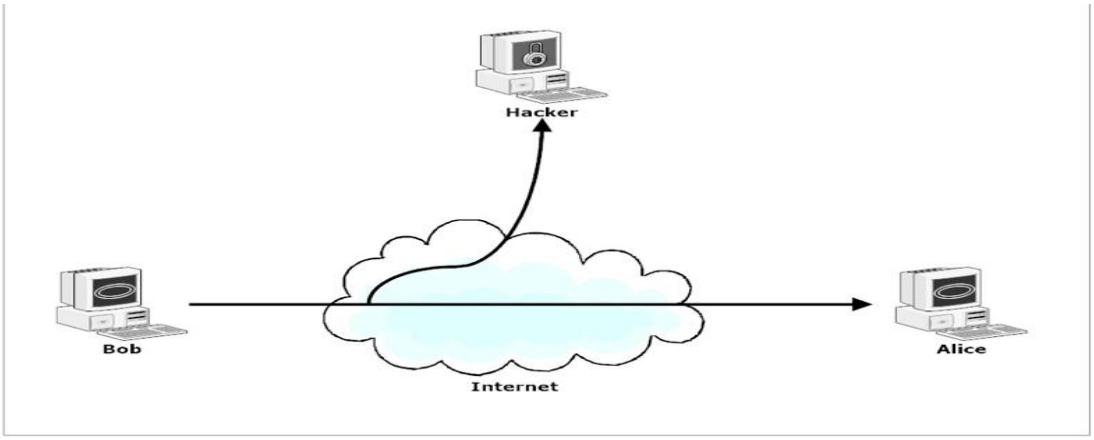


2. PASSIVE ATTACKS

a) **Release of message contents-** For a release of message content, a telephonic conversation, an e-mail message, or a transferred file may contain confidential data. When the messages are exchanged neither the sender nor the receiver is aware that a third party may capture the messages. This can be prevented by the encryption of data. [4]

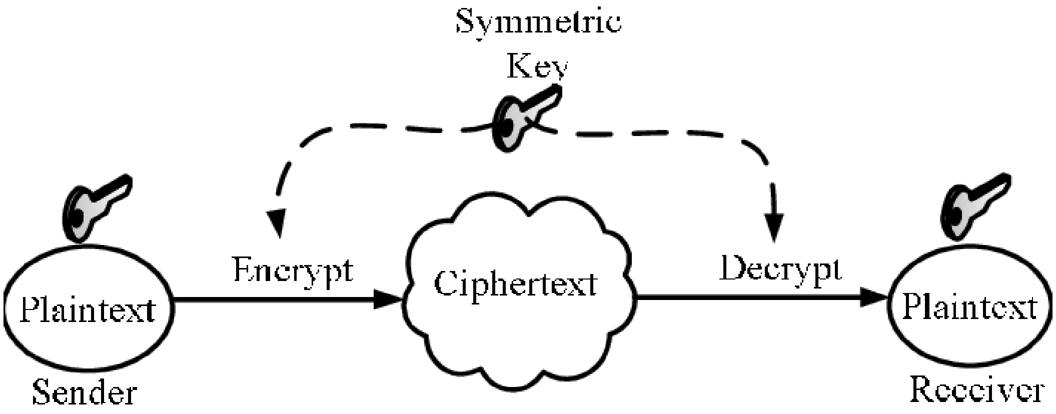


b) Traffic analysis- Traffic analysis is the process of intercepting and examining messages to deduce information from patterns in communication, which can be performed even when the messages are encrypted. [5]

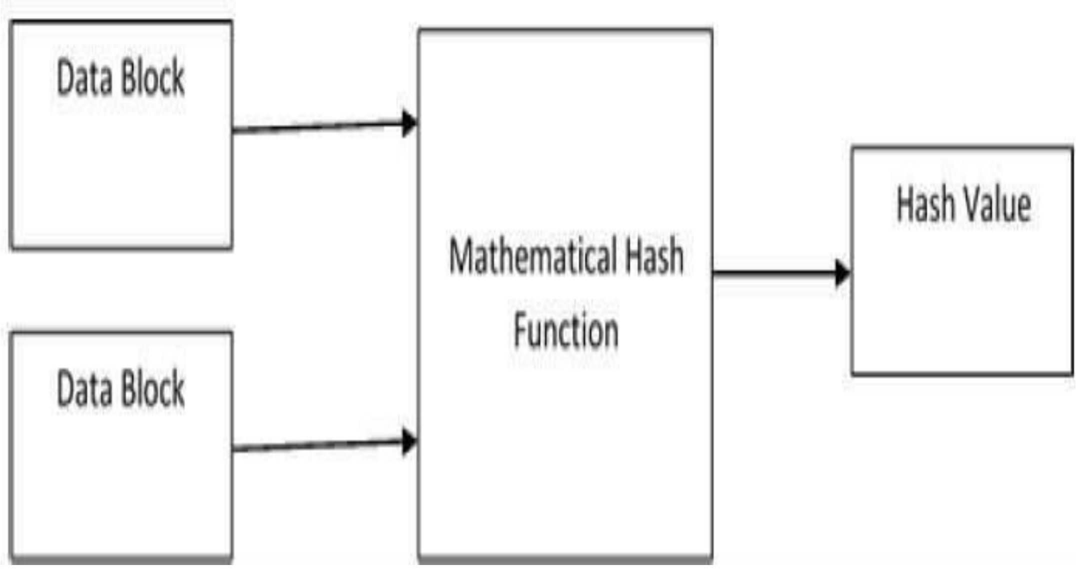


TYPES OF CRYPTOGRAPHY

A. **Symmetric Key Cryptography:** Symmetric encryption is an old technique. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange keys securely.

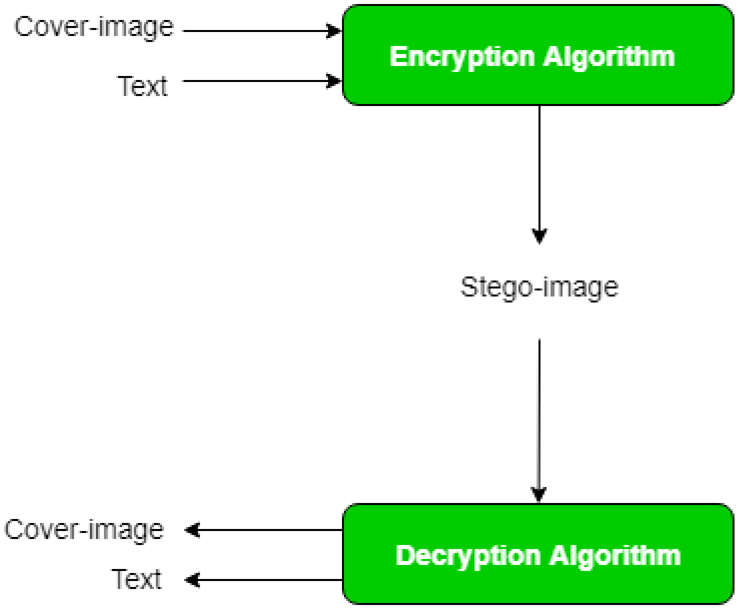


B. Hash Functions: A hash function is a mathematical function that converts a numerical input value into another compressed numerical value and produces a fixed-sized output.



Steganography

Steganography is a method in which a secret message is hidden by text, audio, video, images, network. Steganography is also known as covered writing.



APPLICATION OF CRYPTOGRAPHY

1) Digital Currency
2) E-commerce
3) Military purposes

APPLICATION OF NETWORK SERVICES

1) In-Flight

2) Emergency Response Team
3) App Wall
4) Banking
5) Cloud Malware Protection Service
6) Shopping

CONCLUSION

Today everything is on the internet, thus security plays a very vital role. The older techniques are easy to attack. So, to keep the data secure cryptography is very important to save our data from unauthorized users. The key should be very confidential only to the sender and the receiver. Cryptography is useful for clients for the encryption of information and confirmation of different clients. Some cryptographic algorithms are used in network security to provide secured communication.[6] Cryptography and network security is used in data communication over the internet to provide security.

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%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, and S. Chidambaranathan. "Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs." (2017).