IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025

Cryptography and Network Security

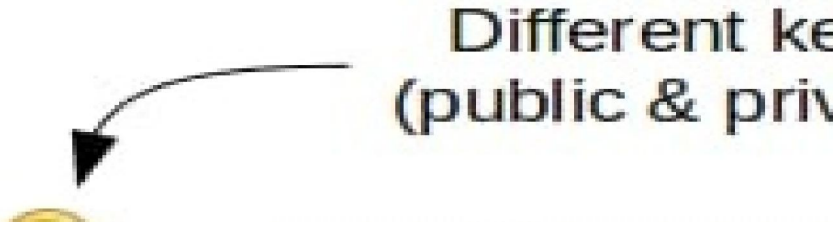
Tanisha Patil, AkankshaPatil, Vaishnavi Joshi
First Year Computer Engineering
Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India

Abstract: *Network Security ensures the safe transmission of data by preventing unauthorized access. It protects both private and public networks, commonly used by organizations, governments, and businesses. Cryptography plays a key role in this by encoding data so only the intended recipient can read it, using techniques like hash functions. This technology, once limited to military and national security, is now widely used in modern communication to secure data and prevent cyberattacks, making it crucial for e-commerce and other applications.*

Keywords: Network Security, Data Transmission, Cryptography, Hash functions, Cybersecurity

I. INTRODUCTION

In today's digital age, network security and cryptography are essential. They shield private data from online dangers and illegal access. Secure communication is ensured via cryptography, which converts plaintext into unintelligible ciphertext. Computer networks are protected from malware, viruses, and hacking via network security. The necessity for secure data transmission has grown as a result of the internet's explosive growth. Network security and cryptography guarantee availability, secrecy, and integrity. They stop identity theft, data breaches, and cyberattacks. Comprehending In today's technologically advanced society, network security and cryptography are essential. They make it possible to communicate, share data, and conduct safe online transactions. Network security and cryptography are necessary for a safe online environment.



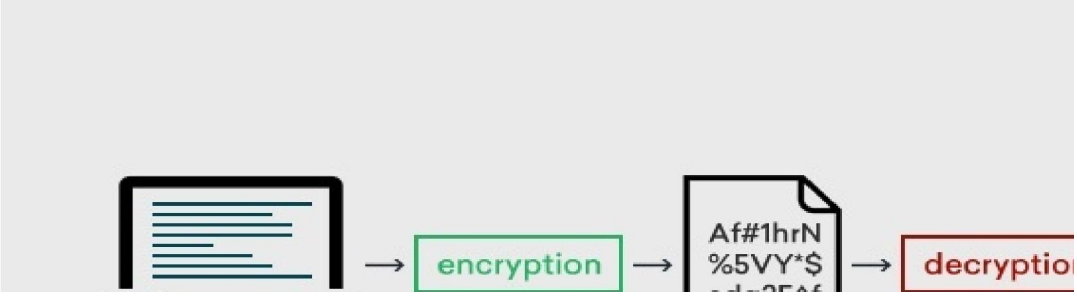
II. METHODOLOGY

A cryptographic technique is defined as a method used to ensure the secrecy and integrity of data in the presence of an adversary. It includes methods like symmetric key cryptography, public key cryptography, and homomorphic encryption to protect data during transportation and storage.

CRYPTOGRAPHY PRINCIPLES

The principles of cryptography are as follows: Hash Functions: Creating digital fingerprints for data; Digital Signatures: Authenticating and verifying message integrity; Secure Key Management: Safely managing encryption keys; Confidentiality: Preventing unauthorised access to data; Integrity: Ensuring data is not altered or tampered with; Authenticity: Confirming sender and recipient identities; Non-Repudiation: Preventing denial of sent or received messages; Key Exchange: Safely exchanging encryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025



CRYPTOGRAPHY GOALS :-

Five primary objectives underpin cryptography:

1. Confidentiality: Guarantees that the message is only comprehensible to the designated recipient.
2. Authentication: Verifies the identity of the sender or recipient.
3. Data Integrity: Verifies that the message was not altered while it was being transmitted.
4. The fourth is non-repudiation, which stops the sender from disputing that they transmitted the message.
5. Access Control: Limits authorised users' access to resources.

ASYMMETRIC CRYPTOGRAPHY

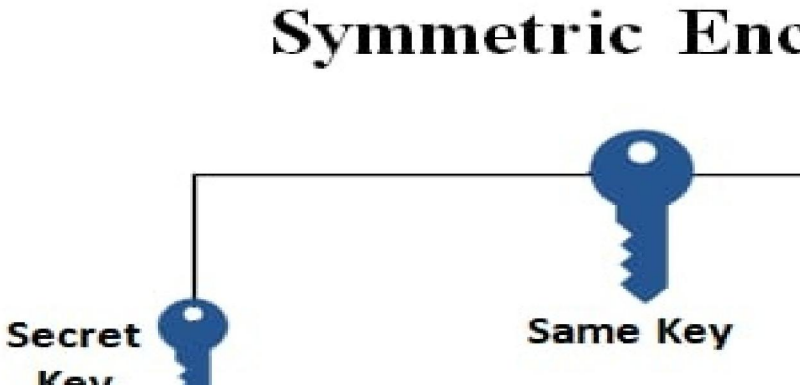
The goals of cryptography and network security are different and asymmetric: confidentiality vs. accessibility: striking a balance between secrecy and availability; security vs. usability: ensuring protection without impeding use; authenticity vs. flexibility: protecting data while permitting legitimate changes; non-repudiation vs. deniability: preventing false denials while permitting plausible deniability; availability vs. stealth: ensuring access while minimising visibility; privacy vs. survey

SYMMETRIC CRYPTOGRAPHY

- Cryptography and Network Security have aligned objectives.
- Confidentiality: Safeguarding sensitive data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025

- Integrity: Maintaining the accuracy and consistency of information.
- Authentication: Confirming identities and sources.
- Availability: Ensuring that authorized users can access resources.
- Non-Repudiation: Preventing denial of performed actions.
- Protection: Defending against unauthorized access.
- Detection: Recognizing potential security threats.
- Prevention: Averting security breaches and attacks.
- Recovery: Reducing damage and reinstating systems after incidents.



ALGORITHIMS IN CRYPTOGRAPHY

Symmetric Key Algorithms

1. AES (Advanced Encryption Standard)
2. DES (Data Encryption Standard)
3. Blowfish

Asymmetric Key Algorithms

1. RSA (Rivest-Shamir-Adleman)
2. ECC (Elliptic Curve Cryptography)
3. Diffie-Hellman Key Exchange

Hash Functions

1. SHA-256 (Secure Hash Algorithm 256)
2. MD5 (Message-Digest Algorithm 5)
3. SHA-1 (Secure Hash Algorithm 1)

Digital Signature Algorithms

1. ECDSA (Elliptic Curve Digital Signature Algorithm)
2. RSA Signature Scheme
3. DSA (Digital Signature Algorithm)

III. CONCLUSION

- Managing vast data volumes and connections from dispersed devices
- Ensuring reliable connectivity, storage, and security

Cloud Computing Solution:

- Scalability and growth in a cloud-based environment
- Lower communication latency and better responsiveness

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025

AWS IoT Security:
- Suite of IoT services with complete security
- Defense in depth approach with multiple security services
- Comprehensive, continuous, and scalable IoT security solutions.

REFERENCES

[1]. https://www.sciencedirect.com
[2]. Itez
[3]. https://aits-tpt.edu.in
[4]. https://docs.aws.amazon.com/whitepapers/latest/securing-iot-with-aws/conclusion.html