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 3, March 2025

Encryption and Decryption

Mrs. N. S. Munde, Abhijeet Gosavi, Aaiyan Shaikh, Kalyani Shinde, Gaurav Vithaldas
Rasiklal M Dhariwal Institute of Technology, Chinchwad, India

Abstract: *In the modern digital era, securing sensitive information is of utmost importance. Encryption and decryption play a crucial role in protecting data from unauthorized access by converting plaintext into unreadable ciphertext and vice versa. Various cryptographic algorithms, such as AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography), are widely used in securing communications, financial transactions, and personal data. This paper explores the fundamental concepts, types of encryptions (symmetric and asymmetric), key management techniques, and real- world applications. Additionally, we discuss emerging threats and advancements in cryptographic techniques, ensuring robust data security in an increasingly interconnected world*

Keywords: Advanced Encryption Standard

I. INTRODUCTION

In today's digital landscape, data security has become a critical concern for individuals, organizations, and governments. Encryption and decryption are essential techniques used to safeguard sensitive information from unauthorized access, cyber threats, and data breaches. Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) using cryptographic algorithms, ensuring confidentiality and integrity. Decryption, on the other hand, is the process of converting ciphertext back into its original form using a decryption key..

In the digital age, protecting sensitive information is crucial to ensure privacy, security, and data integrity. Encryption and decryption are fundamental techniques used to secure data from unauthorized access.

Encryption is the process of converting plaintext (readable data) into ciphertext (unreadable data) using cryptographic algorithms, making it inaccessible to anyone without the proper decryption key. Decryption is the reverse process, converting ciphertext back into its original plaintext form using a key.

Table -1: Sample Table format

Section	Details
introduction	Explanation of encryption and decryption, their importance in data security.
Types of Encryptions	**Symmetric Encryption** **Asymmetric Encryption**
Cryptographic Algorithms	**Block Ciphers** - Encrypts data in fixed blocks (e.g., AES). **Stream Ciphers** - Encrypts data as a continuous stream (e.g., RC4). **Hash Functions** - Used for integrity verification (e.g., SHA-256).
Emerging Trends	Homomorphic Encryption Post-Quantum Cryptography AI-Powered Cryptography

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 3, March 2025

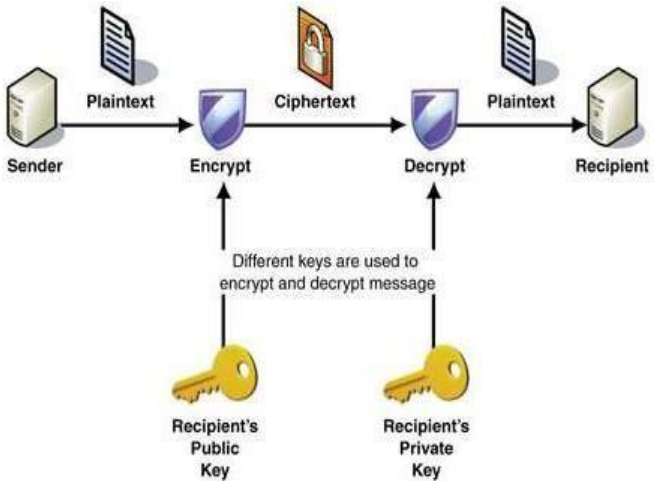

Fig -1: Figure

II. CONCLUSION

Encryption and decryption are essential for securing digital data, ensuring confidentiality, integrity, and authenticity in various applications. From protecting personal communications to securing online transactions and government data, encryption plays a crucial role in modern cybersecurity.

With evolving cyber threats, encryption methods must continuously improve to counter potential risks, including challenges posed by quantum computing and key management issues. Emerging technologies like post-quantum cryptography, homomorphic encryption, and AI-driven security solutions are paving the way for more robust data protection.

As digital dependence grows, individuals and organizations must adopt strong encryption practices to safeguard sensitive information, ensuring a secure and trustworthy digital environment

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to everyone who contributed to the completion of this paper on **Encryption and Decryption**. I extend my heartfelt appreciation to my mentors, teachers, and peers for their valuable guidance, support, and insightful discussions that helped shape this research

REFERENCES

[1]. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
[2]. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
[3]. Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 644-654.
[4]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120- 126.
[5]. National Institute of Standards and Technology (NIST). (2001). Advanced Encryption Standard (AES). Retrieved from https://www.nist.gov
[6]. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press