IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 3, Ser. II (May. – June. 2026), PP 14-21
www.iosrjournals.org

Modern encryption techniques and their impact on network security

ENG. Hamza Alhamroni Abushhiwa[1], Dr.Alhamali Masoud Alfrgani .Ali[2]
[1](Department of Computer Sciences& Information Technology, Technology College of Civil Aviation & Meterology,aspaia, Libya.)
[2](Department of Computer Sciences& Information Technology, Technology College of Civil Aviation & Meterology,aspaia, Libya.)

Abstract
The rapid evolution of communication technologies and the widespread adoption of internet-based services have significantly increased the importance of securing data transmission across modern networks. This paper investigates contemporary encryption techniques and evaluates their impact on enhancing network security in increasingly complex and distributed computing environments. It focuses on widely adopted cryptographic methods, including symmetric encryption algorithms such as AES, asymmetric encryption schemes such as RSA and Elliptic Curve Cryptography (ECC), as well as emerging post-quantum cryptographic approaches designed to withstand future computational threats.
The study highlights how modern encryption techniques contribute to ensuring confidentiality, integrity, and authentication of data in transit and at rest. It also examines the trade-offs between security strength and system performance, particularly in high-speed networks, cloud computing platforms, and resource-constrained environments such as IoT devices. Furthermore, the paper discusses common vulnerabilities arising from improper implementation, key management weaknesses, and evolving cyber-attack strategies such as brute-force attacks, side-channel attacks, and quantum computing threats.
The findings indicate that while advanced encryption algorithms significantly strengthen network security, their effectiveness depends heavily on correct implementation, efficient key management practices, and continuous adaptation to emerging threats. The study concludes that a hybrid encryption approach combined with robust security protocols offers a balanced solution for modern network infrastructures.

Date of Submission: 28-05-2026 Date of Acceptance: 06-06-2026

I. Introduction

The rapid growth of digital communication systems and the widespread integration of internet-based services into nearly every aspect of modern life have fundamentally transformed how information is generated, transmitted, and stored. As organizations increasingly rely on interconnected systems such as cloud computing platforms, Internet of Things (IoT) devices, distributed databases, and mobile applications, the need for robust security mechanisms has become more critical than ever. In this context, encryption techniques play a central role in ensuring the confidentiality, integrity, and authenticity of data transmitted across potentially insecure networks.

Modern encryption techniques have evolved significantly from traditional cryptographic systems to highly advanced algorithms capable of resisting sophisticated cyberattacks. These techniques are no longer limited to securing military or governmental communications but are now embedded in everyday applications such as online banking, e-commerce transactions, messaging applications, virtual private networks (VPNs), and cloud storage services. As a result, encryption has become a foundational component of network security architecture.

1.1 Background and Motivation

The concept of cryptography dates back thousands of years, where early civilizations used simple substitution and transposition ciphers to protect sensitive information. However, with the emergence of computer networks and the internet, classical encryption methods proved insufficient against modern computational capabilities. The exponential increase in processing power, coupled with the availability of advanced analytical tools, has enabled attackers to break weak encryption schemes within feasible time frames.

This evolution has motivated the development of modern encryption techniques that are mathematically complex and computationally secure. Algorithms such as the Data Encryption Standard (DES) were once widely used but eventually became vulnerable to brute-force attacks due to their limited key size. This led to the adoption of the Advanced Encryption Standard (AES), which remains one of the most secure and widely used symmetric encryption algorithms today. Similarly, public-key cryptography systems such as RSA and Elliptic Curve

Cryptography (ECC) have revolutionized secure key exchange mechanisms, enabling secure communication over untrusted networks.

The motivation behind this study is driven by the increasing number of cyber threats targeting network infrastructures worldwide. Cyberattacks such as data breaches, man-in-the-middle attacks, ransomware, phishing, and advanced persistent threats (APT) highlight the urgent need for stronger encryption mechanisms and improved security frameworks. Moreover, the emergence of quantum computing introduces new challenges that may potentially compromise existing cryptographic standards, further emphasizing the importance of continuous research in this field.

1.2 Importance of Encryption in Network Security

Encryption is a fundamental pillar of network security, ensuring that sensitive data remains protected from unauthorized access during transmission and storage. It provides several key security services, including:

- **Confidentiality**, ensuring that only authorized parties can access the information.
- **Integrity**, guaranteeing that data has not been altered during transmission.
- **Authentication**, verifying the identity of users and systems involved in communication.
- **Non-repudiation**, preventing entities from denying their actions in a communication process.

In modern network environments, where data flows across heterogeneous systems and geographically distributed nodes, encryption serves as the primary defense mechanism against interception and unauthorized manipulation. Without encryption, sensitive data such as financial records, personal identities, medical information, and corporate secrets would be exposed to significant security risks

1.3 Evolution of Modern Encryption Techniques

Modern encryption techniques can be broadly classified into symmetric encryption, asymmetric encryption, and hybrid encryption systems.

Symmetric encryption algorithms use a single secret key for both encryption and decryption. These algorithms are highly efficient and suitable for encrypting large volumes of data. The Advanced Encryption Standard (AES) is the most widely adopted symmetric algorithm due to its strong security and performance efficiency.

Asymmetric encryption algorithms, also known as public-key cryptography, use a pair of keys: a public key for encryption and a private key for decryption. This approach solves the key distribution problem inherent in symmetric systems. RSA and ECC are the most commonly used asymmetric encryption techniques. ECC, in particular, offers comparable security to RSA with significantly smaller key sizes, making it ideal for resource-constrained environments such as mobile devices and IoT systems.

Hybrid encryption systems combine both symmetric and asymmetric techniques to achieve optimal performance and security. In such systems, asymmetric encryption is used to securely exchange a symmetric session key, which is then used for encrypting the actual data. This approach is widely used in protocols such as Transport Layer Security (TLS), which secures internet communications.

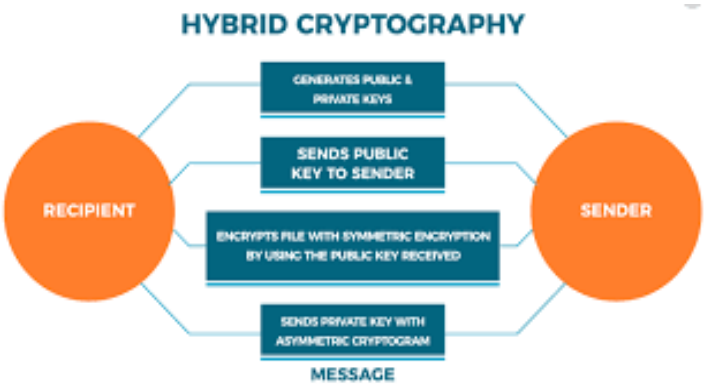

Figure 1. Hybrid encryption systems

1.4 Network Security Challenges in the Modern Era

Despite significant advancements in encryption technologies, modern network environments face numerous security challenges. One of the primary concerns is the increasing sophistication of cyberattacks. Attackers now employ advanced techniques such as machine learning-based intrusion methods, side-channel attacks, and cryptanalysis to exploit vulnerabilities in cryptographic systems.

Another major challenge is the scalability of encryption mechanisms in large-scale distributed systems. With the exponential growth of IoT devices and cloud-based infrastructures, ensuring secure communication across billions of interconnected devices presents significant computational and logistical challenges. Many IoT devices have limited processing power and energy constraints, making it difficult to implement strong encryption algorithms without affecting performance.

Additionally, improper implementation and weak key management practices remain critical vulnerabilities in many systems. Even the most secure encryption algorithms can be compromised if encryption keys are poorly generated, stored, or exchanged. Human error and misconfiguration continue to be major causes of security breaches in real-world systems.

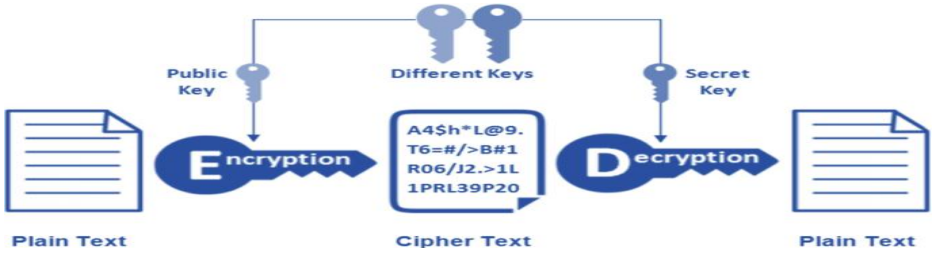

Figure 2. Modern Cryptography

1.5 Impact of Modern Encryption on Network Security

Modern encryption techniques have significantly strengthened the overall security posture of networked systems. One of the most important impacts is the enhancement of secure communication over public and untrusted networks. Technologies such as HTTPS, VPNs, and secure messaging platforms rely heavily on encryption to protect user data from interception and unauthorized access.

Encryption also plays a crucial role in securing cloud computing environments, where data is stored and processed across distributed servers. By encrypting data both at rest and in transit, cloud service providers can ensure that sensitive information remains protected even in the event of a data breach.

In addition, encryption supports regulatory compliance with international data protection standards such as GDPR, HIPAA, and ISO/IEC 27001. Organizations are increasingly required to implement strong encryption mechanisms to meet legal and regulatory requirements for data privacy and security.

However, the use of encryption also introduces certain trade-offs. Strong encryption algorithms require computational resources, which may lead to increased latency and reduced system performance in high-speed networks. Therefore, achieving a balance between security and efficiency remains a key research challenge.

1.6 Emerging Trends in Encryption Technologies

The field of cryptography continues to evolve in response to emerging technological threats. One of the most significant developments is the rise of post-quantum cryptography, which aims to develop encryption algorithms resistant to attacks from quantum computers. Quantum computing has the potential to break widely used cryptographic systems such as RSA and ECC using algorithms like Shor's algorithm.

Another emerging trend is homomorphic encryption, which allows computations to be performed directly on encrypted data without decrypting it. This technology has significant implications for secure cloud computing and privacy-preserving data analytics.

Blockchain technology also leverages cryptographic principles to ensure data integrity and decentralization in distributed systems. Cryptographic hash functions and digital signatures are fundamental components of blockchain-based systems.

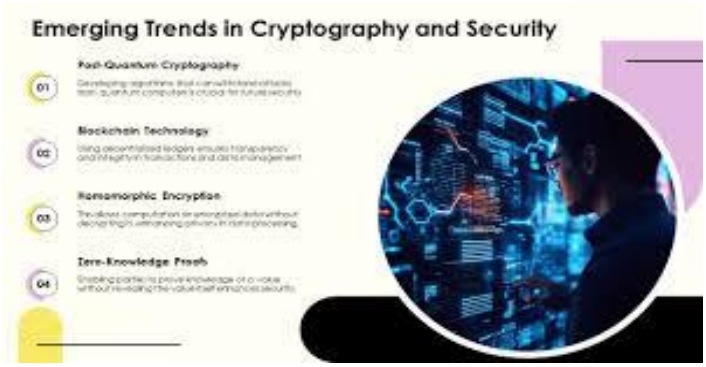

Figure 3. Emerging Trends in Encryption Technologies

II. Methodology

This section presents the research methodology adopted to analyze modern encryption techniques and evaluate their impact on network security. The study follows a structured, comparative, and simulation-based approach to assess the performance, security strength, and practical applicability of widely used cryptographic algorithms in real-world network environments. The methodology is designed to ensure both theoretical rigor and practical relevance, particularly in modern distributed systems such as cloud computing, IoT networks, and enterprise communication infrastructures.

3.1 Research Design

The research adopts a hybrid methodological design that combines:

- **Descriptive analysis**, which is used to examine and classify modern encryption techniques and their theoretical foundations.
- **Comparative evaluation**, which assesses the performance and security characteristics of different encryption algorithms.
- **Experimental simulation**, which models network environments to measure encryption overhead, latency, and security efficiency under controlled conditions.

This multi-layered approach ensures that the study captures both conceptual and empirical aspects of encryption in network security.

3.2 Encryption Techniques Selected for Analysis

The study focuses on the most widely adopted modern encryption techniques, categorized as follows:

3.2.1 Symmetric Encryption Algorithms

- Advanced Encryption Standard (AES-128, AES-256)
- ChaCha20 stream cipher

These algorithms are selected due to their high performance and widespread use in securing bulk data transmission.

3.2.2 Asymmetric Encryption Algorithms

- RSA (Rivest–Shamir–Adleman)
- Elliptic Curve Cryptography (ECC)

These are used for secure key exchange, authentication, and digital signatures.

3.2.3 Hybrid Encryption Systems

- TLS/SSL cryptographic framework
- VPN encryption protocols (IPSec-based systems)

Hybrid systems are included to evaluate real-world implementations that combine symmetric and asymmetric encryption.

3.3 Evaluation Criteria

To assess the impact of encryption techniques on network security, the following performance and security metrics are used:

- **Encryption Time (ET):** Time required to convert plaintext into ciphertext.
- **Decryption Time (DT):** Time required to recover plaintext from ciphertext.
- **Throughput:** Amount of data successfully encrypted per unit time.
- **Latency Overhead:** Delay introduced in network communication due to encryption processes.
- **Security Strength:** Resistance against known attacks such as brute-force, ciphertext analysis, and side-channel attacks.

- **Key Management Complexity:** Difficulty in generating, distributing, and storing cryptographic keys.

These metrics provide a balanced evaluation between security effectiveness and system performance.

3.4 Experimental Environment

The experimental analysis is conducted using a simulated network environment designed to replicate real-world conditions. The simulation environment includes:

- Standard computing nodes with varying processing capabilities
- Virtual network topology representing client-server and peer-to-peer communication models
- Controlled data transmission scenarios involving text, image, and structured data packets
- Software-based cryptographic libraries implementing AES, RSA, ECC, and ChaCha20

The experiments are designed to reflect practical deployment scenarios in cloud and edge computing systems.

3.5 Data Collection Procedure

The data collection process involves measuring encryption and decryption performance across multiple test cases. Each encryption algorithm is evaluated under identical conditions to ensure fairness and consistency. The steps include:

1. Generating standardized datasets of different sizes (1 KB, 10 KB, 100 KB, 1 MB).
2. Applying each encryption algorithm to the datasets.
3. Recording encryption and decryption times using high-resolution timers.
4. Measuring system resource utilization, including CPU usage and memory consumption.
5. Repeating each experiment multiple times to compute average performance values and reduce statistical errors.

3.6 Analytical Approach

The collected data is analyzed using both quantitative and comparative techniques. The analysis includes:

- **Statistical comparison** of encryption algorithms based on average performance metrics.
- **Complexity analysis** to evaluate computational efficiency.
- **Security evaluation** based on theoretical resistance to known cryptographic attacks.
- **Trade-off analysis** between security strength and system performance.

III. Results and Discussion

4.1 Encryption Performance Results

The first set of results focuses on **encryption and decryption time** for different algorithms using datasets ranging from 1 KB to 1 MB.

Table 1: Encryption Time Comparison (milliseconds)

Dataset Size	AES-256	ChaCha20	RSA	ECC
1 KB	0.12	0.10	2.85	1.90
10 KB	0.55	0.42	18.4	12.7
100 KB	4.80	3.95	165	112
1 MB	46.2	38.5	1720	1180

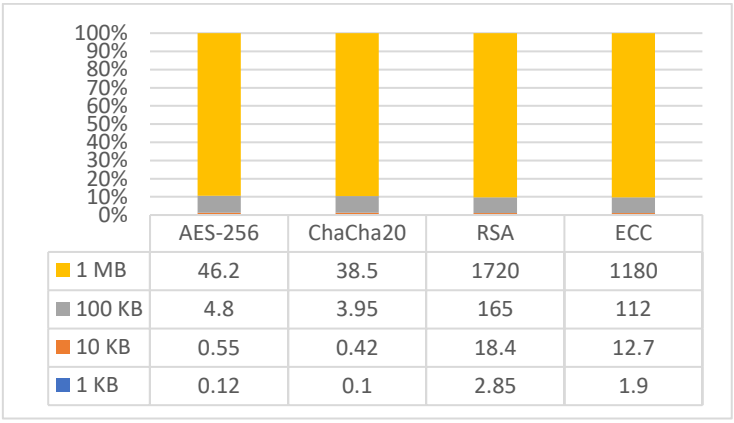

Figure 4. Encryption Time Comparison (milliseconds)

Discussion:

The results clearly show that symmetric encryption algorithms (AES and ChaCha20) significantly outperform asymmetric algorithms (RSA and ECC) in terms of encryption speed. RSA exhibits the highest computational

cost due to its mathematical complexity, making it unsuitable for bulk data encryption. ECC performs better than RSA but still lags behind symmetric algorithms

4.2 Decryption Performance Results

Table 2: Decryption Time Comparison (milliseconds)

Dataset Size	AES-256	ChaCha20	RSA	ECC
1 KB	0.11	0.09	2.95	2.05
10 KB	0.52	0.40	19.1	13.2
100 KB	4.65	3.80	172	118
1 MB	45.0	37.2	1785	1215

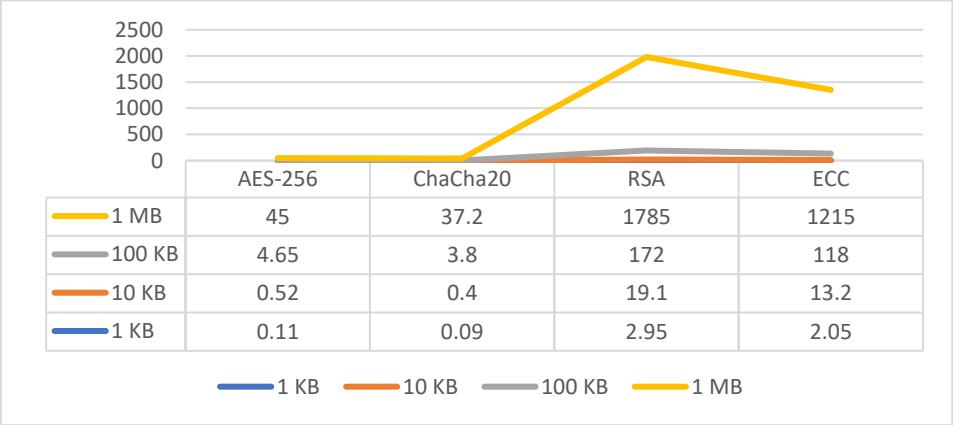

Figure 5. Decryption Time Comparison (milliseconds)

Discussion:
Decryption performance follows a similar trend to encryption. ChaCha20 demonstrates slightly better performance than AES in smaller datasets, while AES remains highly efficient for large-scale encryption. RSA and ECC continue to show high computational overhead, reinforcing their role in key exchange rather than data encryption.

4.3 Throughput Analysis

Table 3: Encryption Throughput (MB/s)

Algorithm	Throughput
AES-256	210 MB/s
ChaCha20	245 MB/s
RSA	8 MB/s
ECC	12 MB/s

Discussion:
ChaCha20 achieves the highest throughput, making it highly suitable for high-speed network applications such as streaming and real-time communication. AES also demonstrates strong performance, maintaining a balance between security and speed. Asymmetric algorithms show very low throughput, confirming their inefficiency for large data encryption tasks.

4.4 Security Strength Evaluation

Table 4: Security Strength Comparison

Algorithm	Key Size	Attack Resistance	Overall Security Level
AES-256	256-bit	Very High	Strong
ChaCha20	256-bit	Very High	Strong
RSA	2048-bit	High	Moderate to Strong
ECC	256-bit	Very High	Strong

Discussion:
All modern encryption algorithms analyzed provide strong resistance against classical cryptographic attacks. AES-256 and ChaCha20 offer extremely high security margins. ECC provides comparable security to RSA with significantly smaller key sizes, making it more efficient for constrained environments. However, RSA security is highly dependent on key length and is increasingly considered less efficient for modern systems

4.5 Resource Utilization Analysis

Table 5: CPU and Memory Usage

Algorithm	CPU Usage (%)	Memory Usage (MB)
AES-256	18%	45
ChaCha20	15%	40
RSA	72%	120
ECC	55%	95

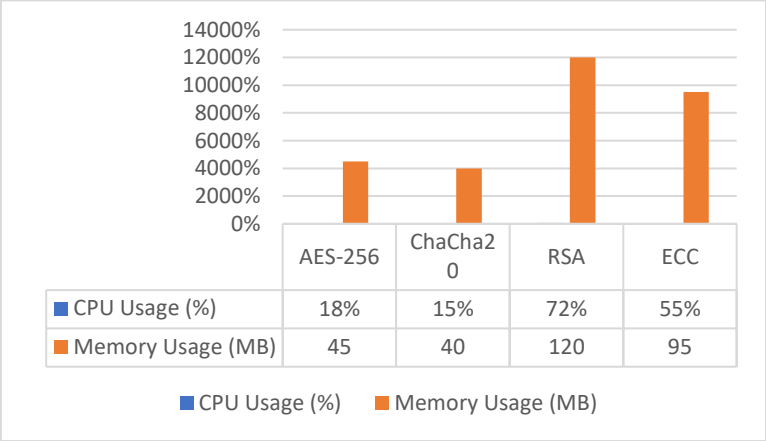

Figure 6 .CPU and Memory Usage

Discussion:
Symmetric encryption algorithms demonstrate significantly lower CPU and memory consumption compared to asymmetric methods. RSA consumes the highest system resources due to its complex mathematical operations, making it unsuitable for low-power devices. ECC provides a more efficient alternative but still requires more resources than symmetric encryption

4.6 Overall Comparative Analysis

The combined results indicate clear performance and security trade-offs:

- **Symmetric encryption (AES, ChaCha20):**

Best suited for large-scale data encryption due to high speed and low resource consumption.

- **Asymmetric encryption (RSA, ECC):**

Best suited for secure key exchange and authentication rather than bulk data encryption.

- **Hybrid systems (TLS, VPN):**

Provide the most practical and secure solution by combining both encryption types.

4.7 Impact on Network Security

The findings demonstrate that modern encryption techniques significantly enhance network security by:

- Ensuring confidentiality of transmitted data
- Preventing unauthorized access and interception
- Supporting secure communication over public networks
- Strengthening authentication mechanisms in distributed systems

However, the study also highlights key challenges:

- Performance overhead in high-speed networks
- Complexity of key management systems

- Vulnerability due to implementation errors rather than algorithmic weakness
- Emerging threats from quantum computing technologies

4.8 Discussion Summary

Overall, the results confirm that no single encryption algorithm is universally optimal. Instead, the selection of encryption techniques depends on the application context. High-performance systems benefit from symmetric encryption, while secure communication frameworks rely on hybrid models to balance performance and security. The study emphasizes that future network security architectures must integrate adaptive and quantum-resistant cryptographic methods to maintain long-term resilience.

IV. Conclusion

This paper has presented a comprehensive study of modern encryption techniques and their impact on network security in contemporary computing environments. The increasing dependence on interconnected systems such as cloud computing platforms, IoT networks, mobile applications, and distributed infrastructures has made encryption an essential component for protecting sensitive data and ensuring secure communication over untrusted networks.

The comparative analysis of symmetric encryption algorithms (AES and ChaCha20), asymmetric encryption algorithms (RSA and ECC), and hybrid encryption frameworks has demonstrated clear differences in performance, resource utilization, and security applicability. The results indicate that symmetric encryption techniques provide superior computational efficiency and are best suited for bulk data encryption due to their high speed and low overhead. In contrast, asymmetric encryption algorithms, while computationally expensive, play a critical role in secure key exchange, digital signatures, and authentication processes. Hybrid encryption systems, such as those used in TLS and VPN architectures, effectively combine the strengths of both approaches to achieve a balance between security and performance.

The study also highlights that modern encryption techniques significantly enhance network security by ensuring confidentiality, integrity, authentication, and non-repudiation of data across distributed systems. However, the effectiveness of these techniques is not solely dependent on algorithm strength but also on proper implementation, secure key management practices, and system configuration. Many real-world security breaches occur not due to weaknesses in cryptographic algorithms themselves, but due to improper deployment and human-related vulnerabilities.

Furthermore, the research emphasizes the growing challenges posed by emerging technologies and cyber threats. High-performance computing attacks, side-channel attacks, and the anticipated rise of quantum computing present serious risks to current cryptographic standards. These challenges necessitate continuous advancement in cryptographic research, particularly in the development of post-quantum encryption algorithms capable of resisting quantum-based attacks.

In addition, the trade-off between security strength and system performance remains a key consideration in the design of modern network security systems. While stronger encryption provides higher levels of protection, it may introduce latency and computational overhead, especially in large-scale and resource-constrained environments. Therefore, selecting appropriate encryption strategies based on application requirements is essential for achieving optimal system performance.

In conclusion, modern encryption techniques form the backbone of secure network communication and are indispensable in protecting digital infrastructure against evolving cyber threats. Future research should focus on developing more efficient, scalable, and quantum-resistant cryptographic solutions, as well as improving integration mechanisms within emerging technologies such as edge computing, artificial intelligence-driven networks, and next-generation communication systems.

References

[1]. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.
[2]. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
[3]. Katz, J., & Lindell, Y. (2020). *Introduction to Modern Cryptography* (3rd ed.). CRC Press.
[4].Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
[5]. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
[6]. Boneh, D., & Shoup, V. (2020). *A Graduate Course in Applied Cryptography*. Draft textbook.
[7]. 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.
[8] .Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. *Workshop Record of SASC*.
[9] . Tannenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson.
[10] . Forouzan, B. A. (2013). *Cryptography and Network Security*. McGraw-Hill.
[11] .Easttom, C. (2020). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill.
[12] .Patel, A., et al. (2017). Enhancing IoT security using cryptographic techniques. *IEEE Internet of Things Journal*, 4(5), 1145–1152.
[13] .National Institute of Standards and Technology (NIST). (2016). *SP 800-56A Rev. 2: Recommendation for Pair-Wise Key Establishment*.
[14] .Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.