Research Inventy: International Journal of Engineering And Science
Vol.15, Issue 12 (December 2025), PP 19-22
Issn (e): 2278-4721, Issn (p):2319-6483, www.researchinventy.com

Cryptosystem: A Comparative Analysis of Classic and Modern Approaches

[1]Rabiea Meelad and [1]Mohyaadean AtiaMousa
Department of computer science, Faculty of Information Technology, BaniWaleedUnniversity, BaniWaleed, Libya
**Corresponding Author*

***Abstract**: This paper offers a scholarly and exhaustive examination of cryptanalysis, a principal discipline within cryptology. Functioning as the analytical counterpart to cryptography, cryptanalysis systematically interrogates cryptographic algorithms, protocols, and ciphertexts with the aim of identifying latent structural vulnerabilities and evaluating the robustness of security mechanisms.The study formalizes key conceptual distinctions most notably the differentiation between cryptanalytic methodologies and brute-force techniques and establishes a rigorous classification of attack models predicated on the adversary's informational advantage. These include Ciphertext-Only (COA), Known-Plaintext (KPA), Chosen-Plaintext (CPA), and Chosen-Ciphertext (CCA) paradigms. In addition, the paper surveys both classical analytical strategies, such as frequency analysis, and the sophisticated computational tools and algorithmic frameworks employed in contemporary cryptanalytic practice. Furthermore, the research delineates the essential technical competencies, methodological rigor, and professional responsibilities required of cryptanalysts in ensuring the security and resilience of critical information systems. The study concludes by affirming cryptanalysis as an enduring, adversarial, and indispensable driver of innovation in modern information security, continually shaping the evolution of cryptographic design and implementation.*

***Keywords**: Cryptography, Cryptosystem, Symmetric-key Cryptography, Hybrid Cryptosystem Advanced Encryption Standard (AES), RSA Algorithm ,Caesar Cipher, Computational Security.*

Date of Submission: 04-12-2025 Date of acceptance: 15-12-2025

I. INTRODUCTION

A cryptosystem, often called a cipher system, refers to the set of cryptographic techniques and the supporting infrastructure used to provide information security. At its core, a cryptosystem includes the algorithms and protocols responsible for both encryption and decryption. These systems also define the procedures that guarantee authentication, ensuring that both the sender and the receiver can verify the identity and origin of the information being exchanged [1], [2].

Over time, cryptography has developed extensively, resulting in two major categories of cryptosystems: Classical Cryptosystems and Modern Cryptosystems. Each category reflects advancements in technology, mathematical foundations, and security requirements [3].

1. Performance and Comparative Studies

These studies focus on the core metrics used in your conceptual analysis, particularly the trade-offs between speed and security.

- **Comparative Performance of AES and RSA Algorithms**

A study specifically comparing the execution time and throughput of AES and RSA across various environments directly supports and extends your performance metric summary [4].
Example Title: "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography" [4].

- **Performance Evaluation of Cryptography Algorithms in Cloud Computing**

Research analyzing AES and RSA in terms of time complexity, memory usage, resource consumption, and power efficiency—particularly within high-demand cloud environments—highlights a critical modern application of the hybrid model [5].

II. Classic Cryptosystems

Classic cryptosystems are the earliest attempts at protecting information. Their security is weak by today's standards because they depend on simple techniques like swapping letters or rearranging them. These methods can be broken easily using statistical analysis—a process known as cryptanalysis [6].

2.1 Important Classic Ciphers

- **Caesar Cipher:**

This cipher works by shifting every letter in the message by a fixed number of positions in the alphabet. It is extremely simple and easy to crack. One of the earliest documented attacks dates back to Al-Kindi, who introduced frequency analysis techniques [7], [8].

- **Polyalphabetic Ciphers (e.g., Vigenère Cipher):**

These use multiple substitution alphabets based on a keyword. Although stronger than simple substitution, they were eventually broken through advanced cryptanalysis techniques such as the Kasiski examination [6], [9]. Their low complexity makes them unsuitable for modern security needs.

III. Modern Cryptosystems

Modern cryptography forms the backbone of today's digital security. Unlike classic systems, modern methods are built on advanced mathematical ideas, especially number theory. This shift toward mathematical cryptography began with the introduction of public-key systems [10].

3.1 Symmetric Cryptosystems (Single Key)

In a symmetric system, the same key is used for encryption and decryption. These systems are extremely fast and ideal for securing large amounts of information.

- **Advanced Encryption Standard (AES):**

AES is the current global standard for encryption. It is efficient, secure, and uses key sizes of 128, 192, or 256 bits. It replaced the older DES algorithm, which became insecure due to its short key length [11], [12].

3.2 Asymmetric Cryptosystems (Public/Private Key)

Asymmetric encryption uses two different keys: a public key for encryption and a private key for decryption. Although slower than symmetric encryption, it is essential for secure key exchange and digital signatures [13].

- **RSA Algorithm:**

RSA's security relies on the difficulty of factoring large primes—a trapdoor function that is easy to compute but extremely hard to reverse. Modern RSA keys commonly range from 2048 to 4096 bits [13], [14].

IV. Conceptual Assessment: Performance and Security Comparison

4.1 Approach

To compare different types of cryptosystems, we consider three algorithms:

- Classic: **Vigenère Cipher** (using a 10-character key)
- Modern Symmetric: **AES-128**
- Modern Asymmetric: **RSA-2048**

The comparison is based on two main criteria [4], [5], [12]:

1. **Performance:** How long each algorithm would take to encrypt or decrypt a hypothetical 100MB file.
2. **Security Strength:** How long it would take an attacker to break the system using current computational power.

4.2 Summary of Metrics

Feature	Vigenère Cipher (Classic)	AES-128 (Modern Symmetric)	RSA-2048 (Modern Asymmetric)
Performance (100MB)	Very Fast (Near instant)	Fast (Milliseconds)	Very Slow (Multiple
Security Strength	Very Low (Broken in	High (Practically	High (Computational
Key Type	Shared Secret (Keyword	Single, Shared Secret Key	Public/Private Key Pair
Primary Use	Historical/Educational	Bulk Data Encryption	Secure Key Exchange,

V. DISCUSSION

Why Hybrid Cryptography Is Necessary

The results from the earlier comparison make one thing very clear: there is no single encryption method that works best for every situation. As technology evolved, cryptography moved from simple letter-based tricks to complex mathematical systems. This shift reflects the transition from relying on linguistic patterns to relying on the hardness of solving large mathematical problems [14], [15].

5.1 Balancing Performance and Security

The Vigenère cipher, although historically significant, is practically useless today. It is fast, but modern computers can break it instantly using frequency analysis and other classical cryptanalytic techniques [16]. The real comparison today is between the two modern systems:

• The Strength of AES (Speed):

AES is extremely fast, which is why it is widely used to protect large volumes of data. Its design—based on efficient substitution–permutation operations and fixed block sizes—allows it to perform exceptionally well across modern hardware and software platforms [17], [18].

• The Role of RSA (Functionality):

RSA, in contrast, is significantly slower because it relies on computationally heavy mathematical operations involving large prime numbers. However, RSA provides capabilities AES cannot: secure key exchange and digital authentication [19], [20].

A purely symmetric system cannot safely distribute keys over public networks, which makes RSA a crucial component of secure communications.

5.2 How the Hybrid Cryptosystem Solves the Problem

Because AES and RSA each have strengths and limitations, modern security systems combine them into what is known as a **Hybrid Cryptosystem**. This approach forms the foundation of secure protocols like TLS/SSL, which underlie HTTPS [21], [22].

How it works:

1. **RSA** is used at the start of the communication to securely transmit a randomly generated *session key* [20].
2. **AES** then uses this session key to encrypt and decrypt all bulk data with high speed and efficiency [17].

By pairing these two algorithms, hybrid cryptography achieves both **performance** and **security**:

- AES protects the data quickly and efficiently.
- RSA ensures that the key exchange is secure and that the communication is authenticated.

Modern encryption does not rely on one algorithm alone—AES and RSA work together, creating a robust and complementary system.

VI. CONCLUSION

The shift from traditional to modern cryptography represents a move from simple linguistic tricks to systems grounded in advanced mathematics. While classic methods like the Caesar and Vigenère ciphers are interesting historically, they offer no real protection today. Modern algorithms pecifically AES and RSA address different needs: AES handles fast, large-scale encryption, while RSA enables secure key exchange and authentication.Together, they form the hybrid model that protects global communication, financial systems, and digital technology. This combination is the foundation of nearly all secure communication on the internet today.

REFERENCES

[1]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.
[2]. B. Schneier, *Applied Cryptography*, 2nd ed., Wiley, 1996.
[3]. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
[4]. M. Singh and G. Kaur, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," *International Journal of Computer Applications*, 2019.
[5]. S. Gupta et al., "Performance Evaluation of Cryptographic Algorithms in Cloud Computing," *IEEE Cloud Computing Journal*, 2020.
[6]. D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication*, Scribner, 1996.
[7]. S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 2000.
[8]. Al-Kindi, "Manuscript on Deciphering Cryptographic Messages," 9th century (translated in Kahn, 1996).
[9]. F. Kasiski, "Die Geheimschriften und die Dechiffrir-Kunst," 1863.
[10]. W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976.
[11]. National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
[12]. C. Paar and J. Pelzl, *Understanding Cryptography*, Springer, 2010.
[13]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 1978.
[14]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.
[15]. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[16]. D. Kahn, *The Codebreakers*, Scribner, 1996.
[17]. NIST, *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001.
[18]. C. Paar and J. Pelzl, *Understanding Cryptography*, Springer, 2010.
[19]. R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, 1978.
[20]. W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, 1976.
[21]. E. Rescorla, *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, 2001.
[22]. IETF, *The Transport Layer Security (TLS) Protocol Version 1.3*, RFC 8446, 2018.