Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.15, No.2, 2025

Application of AES-RSA Hybrid Encryption Technology in Data Transmission Practices

Linyu Ji

School of Information and Security, Yancheng Polytechnic College, No. 285, South Jiefang Road, Yancheng City, Jiangsu Province, 224007, China

* E-mail: Ycjly9970@163.com

Abstract

This study addresses the security risks in computer network data transmission by exploring AES, RSA, and their hybrid encryption techniques. Experimental results demonstrate that the hybrid encryption approach offers superior security and faster encoding/decoding speeds compared to standalone encryption methods.

Keywords: Data encryption, Transmission security, AES encryption, RSA encryption, Hybrid encryption, Collaborative application

DOI: 10.7176/JIEA/15-2-06
Publication date: August 28th 2025

1. Introduction

In the current digital era, the exponential growth of data volume has led to increasingly complex threats in data transmission, including cross-border regulatory requirements and systemic risk proliferation. As a fundamental strategic resource, ensuring data security during transmission is critical for safeguarding personal privacy, corporate competitiveness, and national interests. Data encryption technology converts transmitted information into ciphertext, effectively mitigating risks such as data breaches, unauthorized tampering, and access violations, thereby enhancing transmission reliability while reinforcing confidentiality and attack resistance. Consequently, the optimal selection and refinement of encryption techniques have become a focal point in industry research.

2. Data Encryption Technologies

Data encryption relies on cryptographic principles, employing specific algorithms (e.g., symmetric AES or asymmetric RSA) and keys to transform readable plaintext into unintelligible ciphertext, ensuring confidentiality, integrity, and authentication. The effectiveness of encryption is evaluated based on the difficulty of unauthorized decryption.

2.1 Types of Data Encryption

Common encryption techniques include symmetric encryption, asymmetric encryption, and hash functions.

Symmetric Encryption: uses a single shared key for both encryption and decryption. The sender and receiver must securely exchange this key beforehand [1]. Representative algorithms include the Data Encryption Standard (DES) and Advanced Encryption Standard (AES). The principle is illustrated in Figure 1.

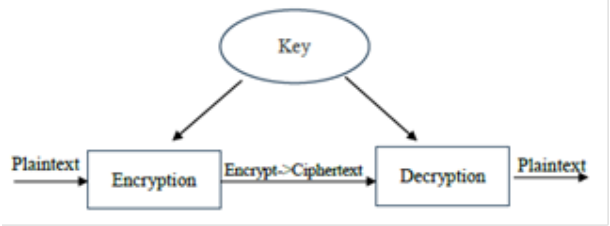

Figure 1 Principle of Symmetric Encryption Technology

Asymmetric Encryption: employs a public-private key pair. The public key encrypts data, while the private key decrypts it, solving key distribution challenges. Examples include RSA and ECC. The principle is shown in Figure 2.

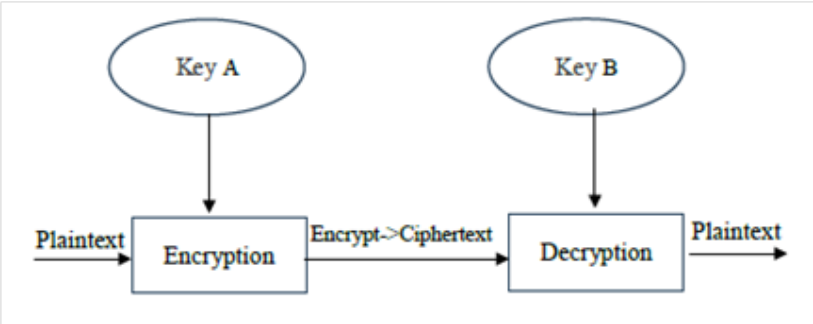

Figure 2 Principle of Asymmetric Encryption Technology

Hash Functions: convert variable-length input into a fixed-length output (hash value). These are irreversible, collision-resistant, and unique, commonly used in digital signatures and message authentication (e.g., MD5, SHA).

2.2 Application Scenarios

In data transmission applications, symmetric encryption algorithms offer several advantages including flexible key management, fast data processing speed, high computational efficiency, low resource overhead, and ease of implementation. These characteristics make them particularly suitable for encrypting massive datasets in big data systems, as well as for real-time applications and high-performance environments such as real-time video streaming and file transfer encryption. However, since the same key is used for both encryption and decryption, the key distribution process presents security vulnerabilities. If intercepted during transmission, attackers could decrypt all communication content. Therefore, practical implementations require careful consideration of mode selection, key management, and channel security to prevent key leakage.

Asymmetric encryption, by contrast, enables secure communication without pre-shared keys, offering higher security at the cost of greater computational overhead. Consequently, it is typically employed only for encrypting small data (e.g., session keys) or digital signatures, rather than for direct encryption of large data volumes. Hash functions are characterized by their one-way encryption process (without decryption capability), and are widely used in security applications beyond integrity verification, including digital signatures, message authentication codes, and pseudorandom number generation.

Each of these cryptographic approaches-symmetric encryption, asymmetric encryption, and hashing algorithms exhibits distinct characteristics in terms of efficiency, security, and applicability. Practical implementations must carefully select the appropriate algorithm based on specific requirements. Detailed comparisons are provided in Table 1.

Table 1. Status of Commonly Used Encryption Technologies

Comparison Dimension	AES	RSA	MD5
Speed/Efficiency	Extremely fast (GB/s)	Slow(MB/s level)	Extremely fast(nanosecond-level)
Security	Relatively high	Very low	Low
Advantages	Good compatibility &supports parallel processing	Wide applicability	Quick verification of data integrity

3. Data Transmission Security Risks

Data transmission security risks refer to potential threats and vulnerabilities arising from malicious attacks, human errors, system failures, or natural disasters that may lead to the theft, leakage, alteration, destruction, or loss of data owned by organizations or individuals. The core concern lies in the compromise of data confidentiality, integrity, and availability.

These security risks can be categorized into five primary types:

Data Breach and Theft: As a core asset and source of competitive advantage, data attracts cyber attackers who employ techniques such as data mining and traffic analysis to exploit vulnerabilities (in software, systems,

networks, or APIs). Through phishing, malware, brute-force attacks, supply chain compromises, and watering hole attacks, they precisely target storage systems and transmission networks to steal government secrets, corporate proprietary data, and citizens' personal information.

Data Tampering: Attackers utilize malicious software including ransomware (which may alter data prior to encryption) and data-corrupting viruses to make unauthorized modifications, rendering data inaccurate, invalid, or maliciously manipulated.

Data Destruction or Loss: Exploiting software flaws or logical errors, attackers deliberately corrupt data, resulting in permanent deletion or irrecoverable inaccessibility.

Data Availability Disruption: Through supply chain attacks or denial-of-service techniques, attackers prevent authorized users or systems from accessing data when needed, even when the data remains physically intact and unbreached.

Data Privacy Violations: Typically resulting from data leaks, insider misuse of access privileges, or flawed data processing workflows (such as excessive collection or insufficient consent mechanisms), these violations involve improper handling (collection, storage, use, or sharing) of personally identifiable information or other private data in violation of legal regulations or organizational policies.

4. Practical Applications of Encryption

4.1 AES-RSA Hybrid Encryption

Recognizing the respective advantages and limitations of symmetric and asymmetric encryption in data transmission, this study proposes an AES-RSA collaborative encryption scheme that achieves an optimal balance between performance and security through the organic integration of both cryptographic techniques. The scheme adheres to the cryptographic principle of "division of labor," employing RSA asymmetric encryption to securely distribute AES keys while utilizing AES symmetric encryption for efficient data protection, thereby effectively overcoming the limitations of single encryption modes. This hybrid architecture not only significantly enhances information confidentiality and transmission reliability but also improves forward secrecy through dynamic key management mechanisms. Having been thoroughly validated in practical applications such as TLS, it provides an innovative solution for establishing highly secure data transmission channels [2]. The technical advantages of this approach are manifested in three dimensions: security (resistance against key leakage attacks), efficiency (high-speed encryption of large data volumes), and extensibility (support for extended functions such as digital signatures), forming a comprehensive end-to-end protection system.

The specific workflow of the AES-RSA hybrid encryption involves: Sender A first encrypts the original data using efficient AES encryption, then encrypts the AES key with the recipient's RSA public key before transmission; Recipient B decrypts the AES key using their RSA private key and subsequently decrypts the data. This design preserves the efficiency of AES in processing large datasets while addressing the key distribution challenge through RSA, effectively defending against security threats such as man-in-the-middle attacks. Currently, this technology is widely applied in scenarios requiring both real-time performance and high security, including HTTPS, VPNs, and financial transactions.

4.2 Efficiency and Security Testing

In data communication systems, ensuring both the security/reliability of encryption/decryption processes and the optimization of computational efficiency are of paramount importance. This study employs a hybrid encryption methodology based on AES and RSA algorithms to protect data during transmission. We conducted comprehensive performance evaluations by measuring the encryption/decryption time for multiple datasets using both symmetric and asymmetric cryptographic algorithms separately. The detailed experimental results are presented in Table 2.

Table 2. Statistics of Encryption and Decryption Test Time

Data Volume	1G	5G	15G
AES-256	2-55	10-255	30-755
RSA-2048	900-12005	4500-60005	13500-180005
Hybrid Encryption	3-65	12-285	33-825

The experimental study employed DES, RSA, and hybrid encryption algorithms to encrypt 200kB data streams.

Utilizing high-performance CPUs and the network packet analyzer Wireshark, we captured encrypted data packets transmitted via FTP protocol. The experimental design incorporated:

i. Ten repeated decryption attempts over a 30-minute duration

ii. Comprehensive brute-force attack simulations

iii. Detailed security analysis of the obtained results

The complete test design and analytical results are systematically presented in Table 3.

Table 3. Brute-force Cracking Cases

Algorithm Type	Cracking Progress within 30 Minutes
AES	Partial exposure of weak keys
RSA	No substantive progress
Hybrid Encryption	Attack completely ineffective

4.3 Full-Lifecycle Data Protection

Comprehensive data encryption throughout its entire lifecycle is achieved via:

i. Transmission Encryption (dynamic protection during data transfer)

ii. Storage Encryption (static protection for data at rest)

iii. Computational Encryption (privacy-preserving computation)

This tripartite approach ensures robust end-to-end data protection [3].

4.3.1 Secure Data Transmission Encryption Protocol

The encryption process for data transmission operates as follows: The sender first generates a random AES key (e.g., AES-256) to encrypt the original data, then encrypts this AES key using the recipient's RSA public key before transmission. Upon receipt, the recipient decrypts the AES key using their RSA private key, then proceeds to decrypt the actual data. This hybrid approach combines the efficiency of AES symmetric encryption (particularly suitable for large-volume data encryption) with the secure key distribution capability of RSA asymmetric encryption. The protocol additionally supports identity verification through digital signatures (as implemented in TLS handshakes), while incorporating forward secrecy (via ECDHE) and authenticated encryption (e.g., AES-GCM) to achieve both high-performance and secure transmission. Furthermore, digital signatures (such as HMAC) are employed to verify data integrity, effectively mitigating man-in-the-middle attacks and replay attacks.

Modern applications including HTTPS and VPNs implement end-to-end protection based on this fundamental principle. For instance:

(1) In tax and social security systems transmitting citizen information, the "RSA-encrypted AES key + HMAC signature" mechanism ensures both data integrity and recipient authentication.

(2) For mobile payment transactions, user payment information is encrypted with AES-256, while sensitive fields like credit card numbers receive additional encryption using RSA public keys. These are then transmitted through PCI-DSS certified terminals to prevent man-in-the-middle interceptions.

4.3.2 Secure Data Storage Encryption Methodology

The data storage encryption protocol implements a hybrid cryptographic approach as follows: Original data (including files or database contents) are encrypted using the efficient AES-256 symmetric encryption algorithm for storage, while the corresponding AES key is asymmetrically encrypted via the recipient's RSA public key and stored separately. The decryption process requires two sequential operations: first, the RSA private key decrypts the AES key; second, the obtained AES key decrypts the actual data.
This dual-layer encryption model delivers three critical security advantages:

i. Performance Optimization: Maintains AES's computational efficiency for large-scale data encryption

ii. Key Management Security: Resolves secure key distribution through RSA cryptography

iii. Access Control Granularity: Enables precise permission management (e.g., restricting decryption capability to RSA private key holders such as administrators)

The methodology finds particular application in Cloud storage services, User file encryption systems,

Transparent Data Encryption (TDE) implementations. These implementations guarantee that even in cases of storage medium compromise, attackers cannot directly access plaintext data.

4.3.3 Computational Encryption

Computational encryption, or privacy-preserving computation, represents a groundbreaking advancement in data security. This technology employs hybrid key management (AES for data encryption + RSA for key protection) throughout the entire workflow, with dynamic decryption strictly limited to authorized scenarios. The core innovation enables direct analysis and computation on encrypted data (e.g., ciphertext retrieval, federated modeling) while ensuring raw data remains protected throughout processing.

Three principal technical approaches achieve this:

i. Homomorphic Encryption: Permits computations on ciphertext, with decrypted results matching those from plaintext operations

ii. Secure Multi-party Computation (MPC): Enables collaborative computation across multiple parties without disclosing individual inputs

iii. Trusted Execution Environment (TEE): Performs isolated computations on decrypted data while maintaining memory encryption

This innovative paradigm effectively addresses the fundamental challenge of achieving "usable yet invisible" data protection, establishing a comprehensive security framework that encompasses: (1) transmission security to prevent eavesdropping, (2) storage protection to prevent leakage, and (3) computational security to prevent exposure. The technology demonstrates particular value in facilitating secure cross-institutional collaboration scenarios, including healthcare joint analysis and financial risk management, where it enables data utility while maintaining strict privacy preservation.

The AES-RSA hybrid encryption framework ("AES for efficient data encryption + RSA for key protection") provides comprehensive lifecycle protection, achieving the "encrypted yet usable and invisible" principle while ensuring complete data transmission security.

4.4 Risks and Optimization Strategies

4.4.1 Security Risk Analysis

The hybrid AES-RSA encryption framework capitalizes on the synergistic advantages of both algorithms, delivering superior performance in efficiency (processing speed), security (robust key distribution), forward secrecy, extensibility, standardization compliance, and broad applicability compared to singular encryption methods. However, this approach still faces notable technical challenges, including key management vulnerabilities (particularly Bleichenbacher attacks against short RSA keys), pseudorandom number generation flaws enabling AES key prediction, susceptibility to side-channel attacks, and the substantial computational overhead associated with homomorphic encryption implementations [4].

4.4.2 Phased Optimization Strategy

Future improvements will be implemented in stages: (1) Short-term (0-18 months): Adopt RSA-3072/AES-256-GCM with hardware security modules for key management and deterministic random number generation; (2) Medium-term (1.5-3 years): Introduce side-channel protections (e.g., masking) and lightweight homomorphic encryption (e.g., BFV) with GPU acceleration; (3) Long-term (3-5+ years): Transition to post-quantum hybrid encryption (RSA+Kyber) while standardizing homomorphic approaches. Concurrently, automated key rotation and zero-trust architectures will be deployed to balance security and efficiency throughout all phases.

5. Conclusion

Data encryption constitutes the fundamental technology of network security, employing sophisticated mathematical algorithms and rigorous implementation protocols to ensure data confidentiality, integrity, and availability. Through continuous optimization of protection mechanisms, diverse encryption algorithms have significantly enhanced communication security, with each technique demonstrating unique advantages in specific application domains. As the foundational safeguard for information security, encryption technologies must still overcome critical developmental challenges. Future advancements require persistent innovation in cryptographic methodologies to effectively counter increasingly sophisticated cyber threats.

References

[1] Lili Huo (2025). Application of Data Encryption Technology in Network Data Transmission [J]. *Technology Innovation and Application*, 13(16): 168-171.

[2] Quan Bin (2024). Application of Hybrid Encryption Algorithm in Computer Network Security[J]. *Electronic Technology*, 53(02): 184-185.

[3] Fu Sunyun (2025). Application of Data Encryption Technology in Computer Network Security Protection [J]. *Information and Computer*, 37(08): 93-95.

[4] Wang Lei (2025). Research on Data Encryption Technology and Its Performance Improvement in Computer Network Security [J]. *China Broadband*, 21(01): 37-39.