COMPARISON OF SYMMETRIC AND ASYMMETRIC ENCRYPTION ALGORITHMS AND THEIR SECURITY LEVEL

Jumaniyozov Firuz
Teacher, department of information security Named after Abu Rayhan Beruni
Urgench State University

Received: 16.10.2025
Revised: 17.10.2025
Accepted: 18.10.2025

Keywords:
cryptography, symmetric encryption, asymmetric encryption, AES, RSA, key exchange, security.

Abstract: This thesis analyzes the theoretical foundations, operating principles, and security levels of symmetric and asymmetric encryption algorithms. The advantages, disadvantages, and practical applications of both approaches are considered. According to the results, symmetric algorithms are superior in speed, while asymmetric algorithms are superior in security for key exchange and authentication.

Introduction. Ensuring information security is one of the most important tasks in the era of digital technologies. Various encryption methods have been developed to maintain the confidentiality of information transmitted or stored over the Internet. The two main types are symmetric and asymmetric encryption. Symmetric encryption uses a single key to encode and decode information. Asymmetric encryption is based on a pair of two keys - a public and a private key. Both methods have their own advantages and can be used together in practical systems.

Features of symmetric encryption

Symmetric encryption algorithms use the same secret key to encrypt and decrypt data. The main advantages of this method are speed and computational efficiency. Symmetric algorithms, such as AES (Advanced Encryption Standard) or Blowfish, encrypt large amounts of data very quickly. Therefore, they are widely used in real-time systems, file systems, and network traffic protection.

However, the biggest drawback of symmetric methods is the key exchange problem. If two users do not securely exchange the same secret key, the entire system is at risk. Therefore, symmetric methods are usually used in local systems or trusted networks.

Characteristics of asymmetric encryption

Asymmetric encryption algorithms are based on two keys — a public key and a private key. The public key is used to encrypt data, and the private key is used to decrypt it. The most popular asymmetric algorithms are RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC).

The RSA algorithm is based on the complexity of factoring large prime numbers, which makes it mathematically very secure. ECC provides a high level of security with a much smaller key size than RSA.

The main advantage of asymmetric encryption is the security of the key exchange. Users send encrypted data using a public key, while the private key is kept only by the owner. Therefore, this method is widely used in digital signature, authentication, and certificate systems.

Comparison and analysis

Symmetric and asymmetric encryption methods are complementary technologies. Symmetric encryption algorithms are fast, consume few resources, and are effective at encrypting large amounts of data. However, their key management is complex, especially when exchanged over networks. Asymmetric encryption solves this problem: users can exchange information securely using a public key. However, this method has high computational complexity, so it is not very effective at directly encrypting large amounts of data.

In practical systems, a hybrid encryption approach is usually used. In this approach, a symmetric key is securely transmitted using an asymmetric algorithm, and then the data is quickly encrypted using a symmetric method. For example, the SSL/TLS protocols are based on these principles.

Conclusion. Symmetric and asymmetric encryption algorithms each play an important role in information security. Symmetric methods are fast and resource-

efficient, while asymmetric methods provide reliable key exchange and authentication. Their combination provides a high level of security and efficiency. In the future, the development of quantum computers will pose a serious threat to current encryption systems. Therefore, the development and implementation of post-quantum cryptography, elliptic curve systems, and hybrid encryption models remain one of the current scientific directions.

References

1. Stallings W. *Cryptography and Network Security: Principles and Practice.* Pearson, 2017.
2. Menezes A., van Oorschot P., Vanstone S. *Handbook of Applied Cryptography.* CRC Press, 1996.
3. Schneier B. *Applied Cryptography.* Wiley, 2015.
4. National Institute of Standards and Technology (NIST). *FIPS PUB 197: Advanced Encryption Standard (AES)* , 2001.
5. Rivest R., Shamir A., Adleman L. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, 1978.
6. Diffie W., Hellman M. *New Directions in Cryptography.* IEEE Transactions on Information Theory, 1976.
7. Koblitz N. *Elliptic Curve Cryptosystems.* Mathematics of Computation, 1987.
8. Boneh D., Shoup V. *A Graduate Course in Applied Cryptography.* 2020.
9. Bernstein D. *Post-Quantum Cryptography.* Springer, 2009.
10. https://en.wikipedia.org/wiki/Public-key_cryptography