Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

# Comparative Insights into State-of-the-Art Cryptographic Techniques and Design Approaches

Most. Mazriha Akter Mohua

World University of Bangladesh

mazriha.akter100212@gmail.com



**Abstract-**The modern communication technology has experienced huge changes with the rapid growth of the Internet. This expansion has made human beings more dependent on it, but has also raised security issues during information exchange. While being transferred over a public network, attackers may monitor and capture the data packets if they are unencrypted. Consequently, the communication process may be interrupted and intercepted. Attackers can combine multiple methods to grab the transmitted data. Therefore, security of information is imperative prior transmission. Cryptography is a security measure to make data unintelligible to intruders. Numerous research studies have been conducted over the decades to introduce a variety of cryptography methods. Several studies have been carried out till this days to determine the optimal encryption method based on specific characteristics, each with its own shortcomings. This prompts individuals to implement robust security measures. This paper provides a comprehensive analysis of contemporary cryptography methods, while also reviewing several existing related research efforts.

**Keywords:** Data Security, Cryptography Algorithm, Symmetric, Asymmetric, Encryption, Decryption.

## I. Introduction

In this modern era, the revolution in communication technology has brought more comfort to the lives of human beings. The Internet is an influential new communication technology that has affected all aspects of human life. As a result, people are spending much of their time on the Internet for various purposes [1]. However, security is a sensitive subject when using the Internet for information transfer because sensitive data may be accessed by unauthorized users connected to the network. Therefore, secure communication requires different levels of security (e.g., computer security, network security) [2]. For providing secure communication and data transmission, cryptography is an essential component used in wireless and wired networks, where private data is converted into an unintelligible form so that intruders cannot access it. The term ‘cryptography’ has a specific meaning in Greek, composed of two words: Kryptos means

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

'confidential' and Graphien means 'writing'. This means cryptography means 'secret writing' [1], [2]. Encryption and decryption are the major functions employed in cryptography [3]. The encryption process obscures the data by converting the plaintext into ciphertext, and the decryption process brings the encrypted data back to its original form. These processes are respectively performed by the sender and the receiver [4], [5].

Cryptographic algorithms' design must be efficient, secure and cost-effective. It should be easily utilized on multiple platforms [2]. With historical roots, cryptography is considered an old technique that is still being developed. To protect data, billions of people across the world use this security measure [5].

## A. Secret Key Cryptography

The symmetric type of cryptography is generally known as SKC (Secret Key Cryptography), which uses a single secret key for both encryption and decryption, as shown in Figure 1(a). Only authorized parties are allowed to possess the key. The strength of SKC depends on the secrecy of the secret key. SKC can be classified into block and stream ciphers based on how message bits are grouped [2]. In a block cipher, a set number of bits are encrypted as a single unit. This means that the plaintext is divided into blocks, encrypted, and then sent to the receiver. On the other hand, a stream cipher operates bit by bit and consists of two components: a key stream generator and a mixing function (XOR function) [2]. There are several symmetric cryptography algorithms available, such as DES, 3DES, AES, Blowfish, etc. [4], [6], [7].

## B. Public Key Cryptography

The asymmetric type of cryptography is known as PKC (Public Key Cryptography), which is used to solve the issue of key distribution. In PKC, a public key and private key are respectively used for encryption and decryption, as shown in Figure 1(b). The public key is known to the public, while the private key is kept secret by the user. Some asymmetric cryptography algorithms are, RSA, ECC, etc. [6], [8], [9].

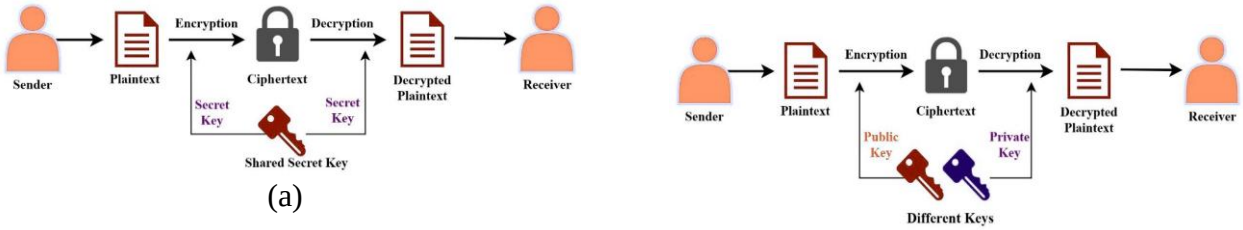


**Figure 1:** (a) Secret Key Cryptography; (b) Public Key Cryptography

# II. State-of-the-Art Cryptography Techniques

### A. DES (Data Encryption Standard)

The symmetric block cipher DES was improved at IBM in 1972 based on the work of Horst Feistel and recommended by NIST. The goal of this algorithm is to provide security to financial databases. DES uses a single key for both encryption and decryption. It includes a 64-bit key, of which 56 bits are directly used by the algorithm as key bits. The remaining 8 bits (parity) are used to detect errors [2], [3]. A 56-bit key encrypts a 64-bit block and then decrypts the resulting 64-bit

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

cipher text using the same key [2], [4]. However, key of smaller size raises vulnerability issues [9].

## B. 3DES

Triple DES was first proposed by IBM in 1998 and standardized in ANSI X9.17 and ISO 8732 [2]. This symmetric technique was created to address the shortcomings of DES [1], [10]. In 3DES, DES algorithm is applied three times to each data block of 64 bits [2]. The key size can be 56, 112, or 168 bits, and 3DES consists of 48 rounds compared to DES's 16 rounds [1].

$$C = Encrypt_{K3}(Decrypt_{K2}(Encrypt_{K1}(P))) \quad (1)$$

$$P = Decrypt_{K3}(Encrypt_{K2}(Decrypt_{K1}(C))) \quad (2)$$

Where C = ciphertext, P = plaintext, and K1, K2, K3 represent the keys. 3DES with three keys requires $2^{168}$ possible combinations, and with two keys requires $2^{112}$ combinations, making it practically impossible to break [1].

## C. AES

Advanced Encryption Standard is a kind of symmetric block cipher introduced in 1997 by the NIST, which is based on the Rijndael cipher. Key sizes, like 128-, 192-, and 256-bit are used in this method. The same key performs both encryption and decryption [4]. AES performs encryption on blocks of 128 bits. The number of rounds in AES are 10, 12, and 14 for the 128-bit, 192-bit, and 256-bit key sizes, respectively. Unlike its predecessor DES, AES does not use a Feistel structure, so it encrypts all 128 bits in one iteration resulting in a comparatively small number of rounds [8], [9]. The data blocks to be encrypted are represented in a matrix referred to as the state array, which changes in every step of the encryption and decryption process. In AES, the steps for each round consist of four layers: substitute byte, shift rows, mix column, and add round key [2], [8], as shown in Figure 3.

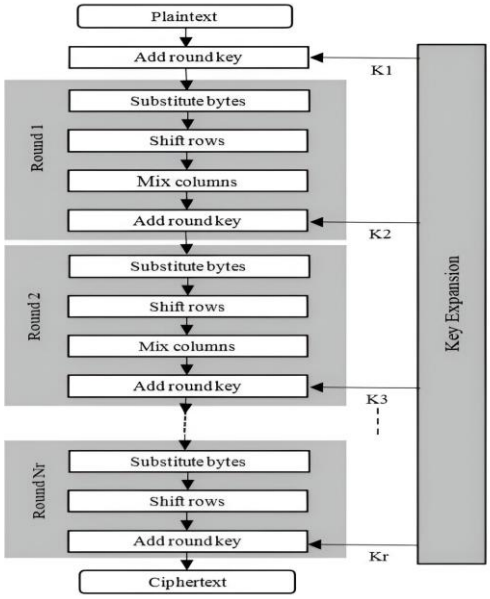


**Figure 3:** AES [2]

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

### D. RSA (Rivest-Shamir-Adleman)

The inventors of asymmetric RSA were Rivest, Shamir, and Adleman, which was invented in 1977. It utilizes public (publicly accessible) and private (secret) keys for encryption and decryption respectively. Since RSA utilizes large prime factorizations, it is effective against attacks [4]. Its key generation involves the following [6], [8]:

1. Take two large prime numbers, p and q.
2. Calculate the modulus, n = pq, and totient function, $\phi(n) = (p - 1)(q - 1)$.
3. Take a prime integer, e ($1 < e < \phi(n)$) and GCD(e, $\phi(n)$) = 1. e = encryption exponent and typically small (65537).
4. Calculate decryption exponent, $d = e^{-1} \bmod \phi(n)$.
5. Obtain the private and public key pairs, (n, d) and (n, e), where n and d are large integers.

Using the public key, RSA generates the cipher text $c = m^e \bmod n$. The plaintext, m, can then be recovered using the private key with the formula $m = c^d \bmod n$ [11].

### E. SHA (Secure Hashing Algorithm)

SHA is a hashing algorithm. SHA-1 has currently been replaced by the stronger SHA-2. SSH, TLS, SSL, etc. applications utilize it. SHA-256, a successor of SHA, produces a fixed-size hash of 256 bits and is suitable for authentication, digital signatures, and other purposes [3].

## III. Literature Review

Several cryptographic algorithms, such as AES, DES, 3DES, Blowfish, RSA, ECC, etc., are available nowadays to ensure information security. Each of these algorithms has its own advantages and disadvantages. However, the choice of the best cryptography algorithm depends on how much security the algorithm can provide, whether it takes optimal computational cost or not, and its applicability in different scenarios [1], [2], [12], [13].

Huge amounts of data are produced daily across the world with the emergence of social networks and commerce applications, making information security a significant issue. Strong cryptography techniques are required with the increase of users connecting to the Internet [14].

Maqsood et al. conducted a review on cryptography and analyzed the performance of several symmetric and asymmetric cryptographic methods by considering execution time, key generation time, and file sizes. The results show that symmetric algorithms are computationally less expensive than asymmetric algorithms [4].

In their review work, Qadir and Varol discussed some of the research conducted in the field of cryptography. The authors also described various historical and modern cryptography algorithms and their applications in various security purposes [5].

Alegro et al. integrated the Schnorr authentication algorithm with AES and RSA to verify users accessing specific information. This authentication method enhances security by reducing the risk of a MITM attack [6]. In other study, the authors have incorporated the Diffie-Hellman key exchange algorithm, RSA, Private Key encryption, SHA-1, and RC5 for enhancing security. They concluded that their approach could offer a superior solution for integrating security policies with LAN-based applications and could serve as an alternative to maintaining security in an intranet [7].In their study, Chaloop and Abdullah proposed a hybrid cryptographic model using AES and RSA. AES encrypts secret data while RSA encrypts the AES key. Experimentation demonstrated that the hybrid mechanism is more reliable compared to using AES or RSA alone. The hybrid

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

algorithm is faster than RSA but slightly slower than AES. Additionally, the throughput of the hybrid mechanism is higher than RSA but lower than AES [15].

## IV. Analysis of Existing Cryptography Methods

A comparative analysis of symmetric, asymmetric, and hashing algorithms is performed in Table I to analyze the characteristics of several cryptography algorithms.

**Table I:** comparative analysis Of existing Cryptographic Techniques

| Algorithm | Type | Contributor (Year) | Block Size (bits) | Key Length (bits) | Rounds | Security | Efficiency |
|---|---|---|---|---|---|---|---|
| DES | SKC | IBM (1977) | 64 | 56 | 16 | Inadequate | Slow |
| 3DES | SKC | IBM (1998) | 64 | 112 or 168 | 48 | Adequate | Fast for hardware |
| AES | SKC | Rijmen and Daeman (2001) | 128 | 128, 192, 256 | 10, 12, 14 | Excellent | Fast |
| Blowfish | SKC | Schneier (1993) | 64 | 32-448 | 16 | Excellent | Fast |
| RC4 | SKC | Ron Rivest (1987) | 2064 | 40-2048 | 256 | Insecure | Fast |
| RC6 | SKC | Ron Rivest et al. (1998) | 128 | 128, 192, 256 | 20 | Good | Fast |
| RSA | PKC | Rivest, Shamir, Adleman (1977) | Variable | 1024-4096 | 1 | Excellent | Slowest |
| ECC | PKC | Victor Miller and Neal Koblitz (1985) | Variable | 160, 192, 224, 256 | 1 | Mostly secure | Fast |
| Diffie-Hellman | PKC | Diffie, Hellman (1976) | Variable | 1024-4096 | 1 | Many attacks | Medium |
| MD5 | Hashing | Rivest (1991) | 512 | 128 | 4 | Insufficient | Fast |
| SHA256 | Hashing | NSA (2001) | 512 | 256 | 64 | Better | Fast |

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

## V. Results and Discussion

The experimental results for DES, Blowfish, AES, and RSA are shown in Table II and Table III, which provide the encryption and decryption times calculated using four different sized input data (e.g., 128-bit, 344-bit, 572-bit, and 678-bit) for each of those cryptography algorithms.

**Table II:** Comparison of Encryption Time of DES, Blowfish, AES, and RSA

| Sl. No. | Data Size | DES Encryption Time (in ms) | Blowfish Encryption Time (in ms) | AES Encryption Time (in ms) | RSA Encryption Time (in ms) |
|---|---|---|---|---|---|
| 1 | 128-bit | 0.16 | 0.29 | 0.57 | 1.14 |
| 2 | 344-bit | 0.47 | 0.52 | 0.91 | 1.65 |
| 3 | 572-bit | 0.76 | 1.54 | 1.67 | 1.98 |
| 4 | 678-bit | 0.97 | 1.78 | 1.97 | 2.54 |

**Table III:** Comparison of Decryption Time of DES, Blowfish, AES, and RSA

| Sl. No. | Data Size | DES Decryption Time (in ms) | Blowfish Decryption Time (in ms) | AES Decryption Time (in ms) | RSA Decryption Time (in ms) |
|---|---|---|---|---|---|
| 1 | 128-bit | 0.27 | 0.79 | 1.74 | 9.94 |
| 2 | 344-bit | 0.79 | 1.32 | 2.04 | 11.36 |
| 3 | 572-bit | 1.28 | 2.03 | 2.59 | 14.47 |
| 4 | 678-bit | 1.66 | 2.89 | 2.88 | 16.77 |

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

It is demonstrated that the encryption and decryption times increase gradually as the input size increases. However, it is evident that DES takes less time for encryption and decryption than the other symmetric algorithms, Blowfish and AES, listed in the table. In addition, RSA takes the longest amount of time for encryption and decryption. As RSA is an asymmetric cryptography algorithm, its decryption time drastically increases.

## VI. Conclusions

This paper provides a comprehensive analysis of the most important state-of-the-art cryptography techniques. Additionally, it reviews related research conducted in the field of cryptography to analyze the performance of existing cryptography methods. AES algorithm has better encryption and decryption time than DES, Blowfish, and RSA. Cryptography ensures reliable and robust data transmission. While both SKC and PKC algorithms have their advantages, the comparison reveals that SKC algorithms prioritize speed over security, whereas PKC algorithms prioritize security over speed. The most suitable algorithm for a specific use varies depending on the requirements. Future work may focus on analyzing additional cryptographic techniques to enhance the performance of existing methods.

## References

**[1]** Salami, Y., Khajevand, V., and Zeinali, E. (2023). Cryptographic algorithms: a review of the literature, weaknesses and open challenges. *J. Comput. Robot*, *16*(2), 46–56.

**[2]** Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., and Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, *8*(11).

**[3]** Hossain, M. A., Hossain, M. B., Uddin, M. S., and Imtiaz, S. M. (2016). Performance analysis of different cryptography algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, *6*(3).

**[4]** Maqsood, F., Ahmed, M., Ali, M. M., and Shah, M. A. (2017). Cryptography: a comparative analysis for modern techniques. *International Journal of Advanced Computer Science and Applications*, *8*(6).

**[5]** Qadir, A. M. and Varol, N. (2019). A review paper on cryptography. In *2019 7th international symposium on digital forensics and security (ISDFS)*, 1–6. IEEE.

**[6]** Alegro, J. K. P., Arboleda, E. R., Perena, M. R., and Dellosa, R. M. (2019). Hybrid schnorr, rsa, and aes cryptosystem. *Int. J. Sci. Technol. Res*, *8*(10), 1777–1781.

**[7]** Agrawal, A. and Patankar, G. (2016). Design of hybrid cryptography algorithm for secure communication. *International Research Journal of Engineering and Technology (IRJET)*,*3*(01), 1323–1326.

**[8]** Mohua, M. M. A., Ameen, A., Saif, A., Aktar, N., and Sakib, M. N. (2025). A novel remote desktop protocol data security approach using hybrid cryptographic algorithm and unsupervised neural network. In *2025 4th International Conference on Computing and Information Technology (ICCIT)*, 377–382, IEEE.

**[9]** Al-Shabi, M. A. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), 576–589.

Received: 2025-07-10
Accepted: 2025-11-26
Published Online: 2025-12-30
DOI: 10.70454/IJMRE.2025.50409

International Journal of Multidisciplinary Research and Explorer (IJMRE)
E-ISSN: 2833-7298, P-ISSN: 2833-7301

**[10]** Anwar, M. N. B., Hasan, M., Hasan, M. M., Loren, J. Z., and Hossain, S. (2019). Comparative study of cryptography algorithms and its' applications. *International Journal of Computer Networks and Communications Security, 7*(5), 96–103.

**[11]** Mohua, M. M. A. (2025). A Review on the Integration of Cryptography and Steganography for Enhanced Information Security. *International Journal of Scientific Research in Multidisciplinary Studies, 11*(8), 51–60.

**[12]** Naeem, B., Senapati, B., Sudman, M. S. I., and AbdelRehim, W. M. (2023). Hybrid architecture for secure data communication within the private cloud.

**[13]** Naidu, D., Tirpude, S., Kalyani, K., Bongir-war, V., and Sharma, T. (2020). Data hiding using meaningful encryption algorithm to enhance data security. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(2), 2408–2413.

**[14]** Tayal, S., Gupta, N., Gupta, P., Goyal, D., and Goyal, M. (2017). A review paper on network security and cryptography. *Advances in Computational Sciences and Technology*, *10(*5), 763–770.

**[15]** Chaloop, S. G. and Abdullah, M. Z. (2021). Enhancing hybrid security approach using aes and rsa algorithms. *Journal of Engineering and Sustainable Development*, *25*(4), 58–66.