Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

REVIEW PAPER ON SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS

POOJA BHATT*
Research Scholar, Department of Applied Mathematics and Computational Science, Shri Govindram Seksaria Institute of Technology and Science, Indore, Madhya Pradesh, India.
*Corresponding Author Email: bhattpooja276@gmail.com

RACHNA NAVALAKHE
Associate Professor, Department of Applied Mathematics and Computational Science, Shri Govindram Seksaria Institute of Technology and Science, Indore, Madhya Pradesh, India.
E-mail: sgsits.rachna@gmail.com

Abstract

Symmetric cryptographic algorithms, also known private-key algorithms, these are single shared key algorithms for both encrypting and decrypting data. Asymmetric cryptographic algorithms, also known as public-key algorithms use a pair of public and private keys, are mathematically related with each other. Both the keys are related to each-other but mathematically impracticable to attain one key from the other. In this paper, we compare Symmetric and Asymmetric key algorithms with respect to time, security level, classification of the data, key length and key management. Moreover, we perform a crisp analysis of cryptographic algorithms with various advantages. Lastly, we conclude a set of recommendations for selecting the correct cryptographic algorithm with applicable 'Use Case' for secured communication.

Keywords: Symmetric and Asymmetric Key; Cryptographic Algorithms; Hybrid Cryptography; Confidentiality and Security; Key Exchange Protocol.

1. INTRODUCTION

Cryptography is the process of reducing plaintext into ciphertext and vice versa for the security while communicating in the presence of third parties or adversaries. Cryptographic algorithms are the sequenced set of instructions or rules used to writing and solving the codes to convey the information securely.

These algorithms are prepared to convert data into a secure format (encryption) and then back into its original form (decryption) using cryptographic keys. The keys are either symmetric or asymmetric and also most important part of cryptography.

Cryptographic algorithms performs in various field of information security, including:

I. **Confidentiality:** Ensuring that the data is protected from unauthorized parties.
II. **Integrity:** Assuring that data has not been modified, inserted, deleted, replayed or fiddled with throughout the communication or storage.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

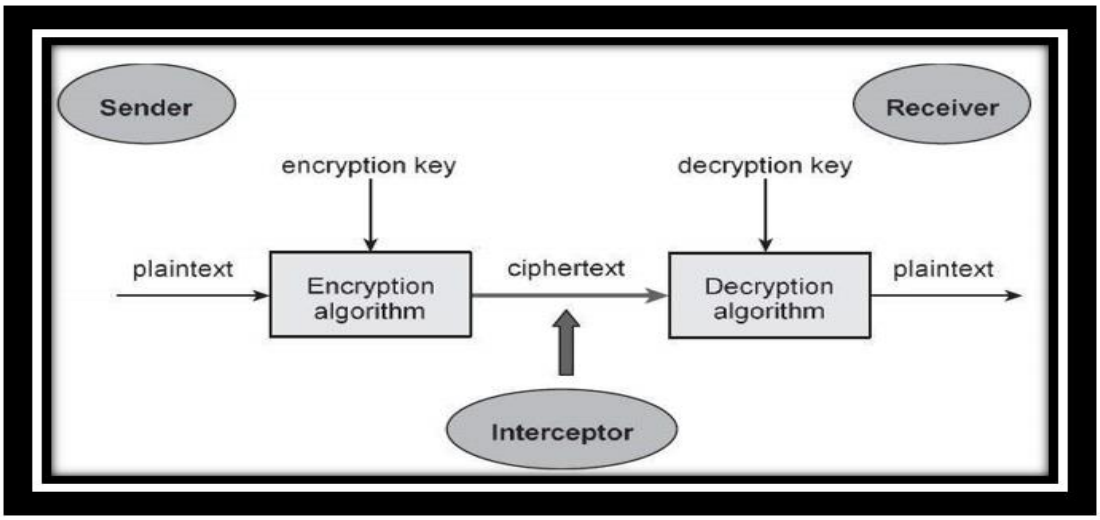

Fig 1.1: Caption: Concept of Cryptography

Fig. 1.1 Alt Text: A padlock symbolizing secure data, surrounded by cryptographic algorithms and key symbols. The padlock signifies the encryption of information for enhanced security, while the algorithms and keys highlight the intricate processes involved in securing and decrypting data in the field of cryptography.

III. **Authentication:** Confirming the identity of communicating entity to ensure that they are who they are claiming.

IV. **Non-Repudiation:** Preventing the denial of having participation by the involved parties.

V. **Key Exchange:** Providing the safe exchange of cryptographic keys between sender and receiver for maintaining confidentiality and security of data.

Common cryptographic algorithms 1) include:

- **Symmetric Key Algorithms:** Examples include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES. These are single shared key algorithms for both encryption and decryption.
- **Asymmetric Key Algorithms:** Examples include Elliptic Curve Cryptography (ECC) and RSA (Rivest-Shamir-Adleman). These algorithms use a pair of public and private keys, are mathematically related with each other.
- **Hash Functions:** Examples include SHA-256 (Secure Hash Algorithm 256-bit) and MD5 (Message Digest Algorithm 5). Hash functions generate a fixed-size hash value from input data, commonly used for data integrity verification.
- **Key Exchange Algorithms:** Examples include Diffie-Hellman key exchange 6), in which two entity agree on a shared secret over an insecure user interface.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

It's important to acknowledge that the selection of cryptographic algorithm based on the precise security prerequisites of a certain system, the danger landscape, and the performance limitations. Security professionals and cryptographers continuously assessing and upgrading cryptographic algorithms to handle new threats and technological development 2).

2. SYMMETRIC KEY ALGORITHMS

Symmetric cryptographic algorithms, also known as symmetric-key algorithms, are the algorithms in which only one secret key is used for both encryption and decryption of data. In other words, the sender and the receiver share a secret key that is used to both encode and decode the information. The foremost motive of symmetric cryptography is to assuring the security and reliability of the data being transmitted or stored.

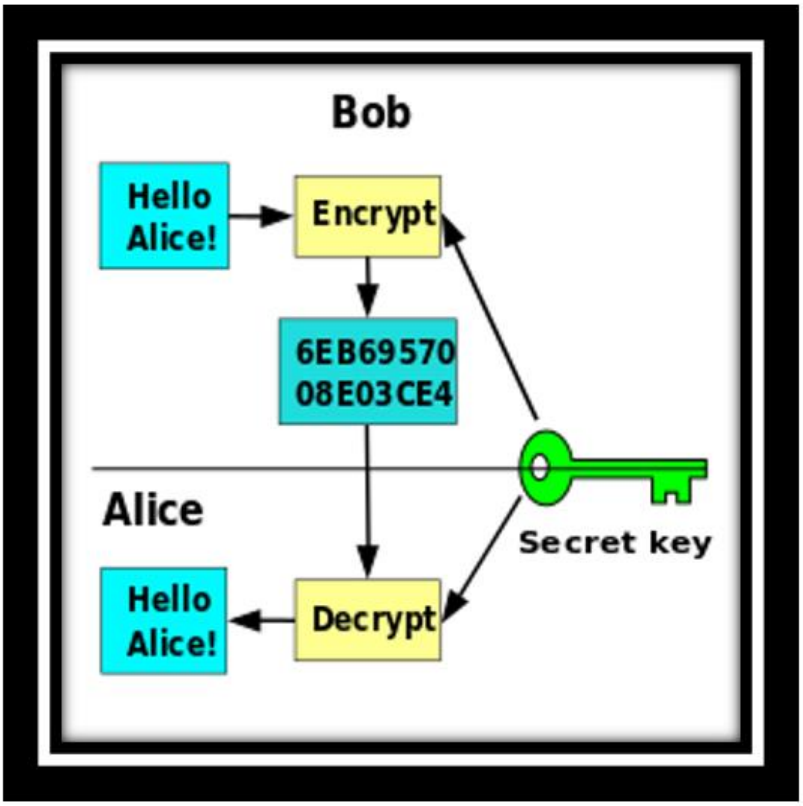

Fig 2.1: Caption: Symmetric Key Cryptography

Fig. 2.1 Alt Text: Two interconnected padlocks symbolizing the use of a shared secret key for both encryption and decryption processes. The symmetric key, represented by the link between the padlocks, emphasizes the reciprocity in securing and accessing information, characteristic of symmetric cryptographic algorithms.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

Here's a basic components of symmetric key cryptography:

I. **Key Generation:** A secret key is generated using key generation algorithm 4). Only communicating parties are aware of this key and also this key is kept confidential.

II. **Encryption:** The generated secret key is applied on the plaintext (original message) with the help of encryption algorithm to get ciphertext (encrypted message). The process of converting plaintext to ciphertext is known as encryption 5).

III. **Decryption:** The same generated secret key is applied by receiver on ciphertext produces the original message with the help of a decryption algorithm. This process is called decryption.

Confidentiality of the private key is essential for the security of symmetric-key algorithms. If a third party knows the key, they can decode the coded text and jeopardized the confidentiality of the communication. Therefore, key management is an essential component of symmetric cryptography 7).

Common symmetric-key algorithms include:

I. **Advanced Encryption Standard (AES):** AES works on fixed-size blocks of data and supports key sizes of 128, 192, or 256 bits. Mostly used and considered secured.

II. **Data Encryption Standard (DES):** Uses a 56-bit key, an older symmetric encryption algorithm. While DES was considered mostly used, its key length is now considered too short for robust security, and therefore it has been replaced by more secured algorithms like AES.

III. **Triple DES (3DES):** 3DES is more secure than DES but is also considered somewhat outdated. A variation of DES that smears the DES algorithm thrice to each data block, using two or three different keys.

Symmetric cryptography is widely employed for securing communication channels and safeguard data at rest. However, a problem with symmetric cryptography is key distribution – making sure that both the parties safely share the secret key without it being intercepted by outsider entities. To solve this problem Public-key cryptography introduced a couple of keys, one public and one private, but it is often requires complex powered computation and more intensive than symmetric-key cryptography. As a result, a blend of both symmetric and asymmetric cryptography is often used in modern cryptography to get more efficient and secured systems.

3. ASYMMETRIC KEY ALGORITHMS

Asymmetric cryptographic algorithms 8), also often considered as public-key algorithms, use a couple of distinct but linked keys for encryption and decryption. Contrast symmetric key algorithms, where for both encryption and decryption same key is used, asymmetric algorithms uses a public key for encryption and a private key for decryption (or vice versa).

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

The public and private keys are mathematically connected but computationally impossible to achieve one with the help of other.

Here's a basic overview of how asymmetric key cryptography works:

I. **Key Pair Generation 23):** A couple of keys – public key and private key are generated. The public key can be established independent for the distribution and the private key must be kept confidential.

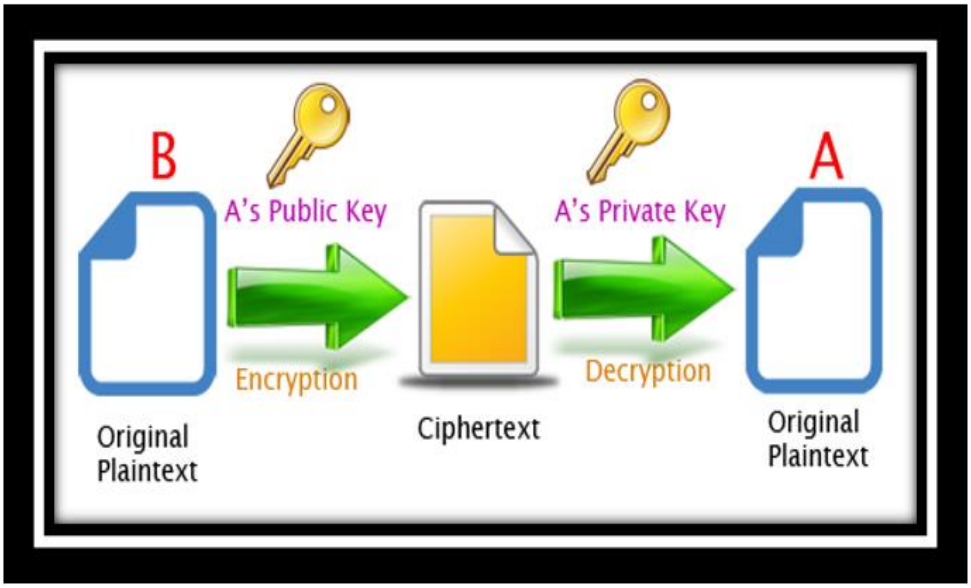

Fig 3.1: Caption: Asymmetric Key Cryptography

Fig. 3.1 Alt Text: Two distinct but mathematically linked keys, portrayed as a padlock and an open lock. The padlock signifies the public key, while the open lock represents the private key. This illustrates the unique key pair characteristic of asymmetric cryptography, enhancing data security through separate keys for encryption and decryption processes.

II. **Encryption:** If we need to communicate an enciphered message to the owner of the key pair, then we have to use the receiver's public key to convert the original message in coded form. After encryption, only the paired private key can reveal the original message.

III. **Digital Signatures:** on the other hand, if the owner of the key pair want to digitally sign a message to show its authenticity, they create a digital signature using their private key. Any person with access to the paired public key would be able to verify the signature and make sure that the message has not been fiddled with.

The sanctuary of asymmetric key cryptography is achieved on the basis of mathematical complexity of certain computational problems, for example factorisation of large numbers.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

Common asymmetric cryptographic algorithms include:

I. **RSA (Rivest-Shamir-Adleman):** It is considered as one of the initial concrete public-key algorithms, RSA is mostly used for protected communication and digital signatures 10). It is based on the complexity of factorisation of the product of two large prime numbers.

II. **Elliptic Curve Cryptography (ECC):** ECC gives more safety with lesser key lengths related to other asymmetric algorithms, making it predominantly suitable for resource-compelled surroundings. ECC is achieved using elliptic curves mathematics over finite fields.

III. **Diffie-Hellman Key Exchange:** While it is not the algorithm used for encryption, but Diffie-Hellman is an algorithm to exchange key that allows receiver and sender to settle on a shared secret over an insecure channel. Then parties can use shared secret as a symmetric key for further transmission of messages 6).

Asymmetric cryptography discourses many of the key management challenges related to symmetric key cryptography. The public keys can be set freely for distribution and can be employed by anyone to encode messages or authenticate digital signatures, while the private keys must be kept confidential. This make sure the key distribution more secured, forthright and enables functionalities like safety, security, authenticity and data integrity. Though, asymmetric cryptography is usually more computationally complex than symmetric cryptography, so it is widely applied in combination with symmetric algorithms to establish a balance of performance and security in cryptographic systems.

4. COMPARISON

Symmetric and asymmetric cryptographic algorithms have dissimilar pros and cons, and each is suitable to different use cases. Here's a comparison of the two:

I. Key Management:

- **Symmetric:** This needs a secure channel for exchanging and managing secret keys. If an unsanctioned party is able to entree to the key, they can decode the communication easily.
- **Asymmetric:** managing key is easier because each user has a pair of public and private keys. Public keys can be established independent for distribution, and private keys must be kept confidential.

II. Computational Efficiency:

- Symmetric: Typically faster and computationally more capable than asymmetric algorithms. Efficient for encrypting huge volume of data.
- Asymmetric: Typically gradual than symmetric algorithms due to more multifaceted mathematical operations. Often employed for key exchange, digital signatures, and smaller amounts of data.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

III. Security:

- Symmetric: offers robust security until the key is kept confidential. Susceptible to key distribution challenges.
- Asymmetric: Depends on mathematical problems (e.g., factoring large numbers, elliptic curve discrete logarithm) for security. Usually considered more secure for key exchange and digital signatures.

IV. Key Length:

- Symmetric: Entails shorter key lengths for equivalent security compared to asymmetric algorithms. AES, for example, can provide strong security with key lengths of 128, 192, or 256 bits.
- Asymmetric: Requires longer key lengths for equivalent security. RSA, for instance, often uses key lengths of 2048 bits or more.

V. Use Cases:

- Symmetric: Seemly for encrypting large amount of data and guaranteeing confidentiality. Generally used in bulk data encryption, such as secure communication channels and disk encryption 11).
- Asymmetric: Widely employed for key exchange, digital signatures, and scenarios where secure communication channels need to be achieved over unsecured channels.

VI. Performance:

- Symmetric: Generally performs comparatively better in terms of speed and efficiency for encryption and decryption.
- Asymmetric: Weaker performance, especially for large-scale data encryption. More computationally rigorous 13).

VII. Examples:

- Symmetric: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES).
- Asymmetric: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) 20), Diffie-Hellman.

VIII. Hybrid Cryptography:

- Combination: Widely, a merger of both symmetric and asymmetric cryptography is employed to pull the strengths of each. For example, asymmetric algorithms is used for key exchange and symmetric algorithms for data encryption.

Amalgamation of symmetric and asymmetric algorithms results in optimized performance, security, and key management.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

Here's a simplified comparison table between symmetric and asymmetric cryptographic algorithms based on time, security, and classification of data 19):

Table 4.1: Comparison between Symmetric and Asymmetric Algorithms

Criteria	Symmetric Algorithms	Asymmetric Algorithms
Time (Computational Efficiency)	Typically quick and computationally efficient. Suitable for bulk data encryption.	Slower than symmetric algorithms due to difficult mathematical operations. Appropriate for key exchange, digital signatures, and smaller data sets.
Security	Offers robust security as long as the key must be kept confidential. Susceptible to key distribution challenges.	Depends on mathematical problems for security, often considered more secure for key exchange and digital signatures.
Classification of Data	Appropriate for encrypting huge data and make sure confidentiality.	Widely used for key exchange and scenarios where secure communication channels are established over unsecured channel.
Examples	AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple DES).	RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), Diffie-Hellman.
Key Length	Entails shorter key lengths for equivalent security.	Requires lengthier key lengths for equivalent security.
Key Management	Requires secure methods for distributing and managing secret keys.	Simpler key management as each user has a pair of public and private keys.
Performance	Offers better performance in terms of speed and efficiency for encryption and decryption.	Slower performance, especially for large-scale data encryption.
Hybrid Cryptography	Often used in combination with asymmetric algorithms for key exchange and symmetric algorithms for data encryption.	Commonly integrated to optimize performance, security, and key management.

It’s completely depends on certain requirements of a given cryptographic application whether to use symmetric or asymmetric cryptography. Many systems use a hybrid method 16) to pull the benefits of both types of algorithms.

The comparison among DES, 3DES, RSA, AES, BLOWFISH and ECC on the basis of Scalability, Encryption and Decryption Speed, Security and Inherent Vulnerabilities is mentioned below 22).

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

Table 4.2

Algorithm	Scalability	Encryption and Decryption Speed	Security	Inherent Vulnerabilities
RSA	Not Scalable	High	Least Secure	Forced and Oracle attack
DES	Scalable	Low	Not Secured Enough	Brute Forced, Linear and differential Cryptanalysis attack
AES	Not Scalable	Low	Excellent Secured	Brute Force Attack
3DES	Not Scalable	Low	Excellent Secured	Meet-in-the-middle-attack
BLOWFISH	Scalable	Low	Least Secure	Birthday Attack
ECC	Scalable	Low	Average Secured	Brute Force Attack

5. USE CASE, ADVANTAGES AND CONSIDERATIONS

The selection of correct cryptographic algorithms depends on various features, including the specific use case, security requirements, and the nature of potential threats. As we know that the domain of cyber-security is dynamic, and new developments may have occurred since recent update. Here are some general considerations:

I. Symmetric Algorithms (e.g., AES):

- **Use Case:** Symmetric algorithms like Advanced Encryption Standard (AES) are suitable for encrypting large volumes of data and ensuring confidentiality.
- **Advantages:** They provide quick and proficient encryption and decryption processes, making them appropriate for larger data encryption.
- **Considerations:** Managing key is vital. Safeguard and secured distribution of the secret keys is necessary to upholding the security of the system.

II. Asymmetric Algorithms (e.g., RSA, ECC):

- **Use Case:** Asymmetric algorithms are widely employed for key exchange, digital signatures, and scenarios where secure communication channels need to be achieved over unsecured channels.
- **Advantages:** Offers a secure way for entities to exchange keys without requiring a pre-established shared secret.
- **Considerations:** Asymmetric algorithms tend to be slower than symmetric ones. The key lengths used in asymmetric cryptography should be chosen carefully to fight potential threats, considering the current state of computational power.

III. Hybrid Cryptography:

- **Use Case:** most of modern cryptographic systems use hybrid algorithms which is a blend of symmetric and asymmetric algorithms (hybrid cryptography) to attain the fortes of both.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

- **Advantages:** Efficient key exchange through asymmetric algorithms and fast data encryption with symmetric algorithms.
- **Considerations:** Need vigilant design and implementation to make sure complete security. Proper key management remains decisive.

IV. Elliptic Curve Cryptography (ECC) 20):

- **Use Case:** ECC is getting fame due to its ability to deliver more security with short key lengths paralleled to traditional asymmetric algorithms 9).
- **Advantages:** Efficient use of computational resources, making it appropriate for resource-compelled surroundings such as IoT devices.
- **Considerations:** The choice of ECC or other asymmetric algorithms depends on factors like performance requirements and the computational capabilities of the devices involved.

V. Post-Quantum Cryptography (PQC):

- **Considerations:** As the era of quantum computers predicted nearer, there is open-ended research in post-quantum cryptography. Algorithms resilient to attacks by quantum computers are being explored as a long-term security solution.

6. CONCLUSION

In modern cryptography, the most indispensable challenges are methods for the generation of key, exchange of key, encryption and decryption and deliver safekeeping depending on the powered key and the robust cryptographic system used. In this paper, cryptographic algorithms are analysed and compared. Lastly, recommendations made on the basis of necessities of the implication based on choice of appropriate encryption techniques. Strategic foresight to this work can be the insertion of a new public key cryptography and hybrid cryptographic method which is stronger in Quantum Cryptography 19).

References

1) A. Joseph Amalraj, D. J. J. R. J., 2016. A Survey Paper On Cryptography Techniques. *International Journal of Computer Science and Mobile Computing,* 5(8), pp. 55-59.

2) Abdalbasit Mohammed Qadir, N. V., 2019. A Review Paper on Cryptography. *IEEE Conference Paper.*

3) Abobala, M. M. a. M., 2023. Research Article On Some Novel Results about Split-Complex Numbers, the Diagonalization Problem, and Applications to Public Key Asymmetric Cryptography. *Hindawi Journal of Mathematics,* p. https://doi.org/10.1155/2023/4481016.

4) Albudawe, A. B. H. a. I. O., 2017. Encrypt and Decrypt Messages Using Invertible Matrices Modulo 27. *American Journal of Engineering Research (AJER),* 6(6), pp. 212-217.

5) Ayush Mittal, D. R. K. G., 2020. Encryption and Decryption Scheme Involving Finite State Machine and LU and Decomposition. *Journal of Xi'an University of Architecture and Technology,* 12(2), pp. 1270-1285.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 01 | 2025
DOI: 10.5281/zenodo.14744308

6) Diffie, W. &. H. M., 1976. New directions in cryptography. 22, 644-654(6).

7) Huawei Huang, C. L. a. L. D., 2022. Public-Key Cryptography Based on Tropical Circular Matrices. *applied sciences (MDPI),* p. https://doi.org/10.3390/app12157401.

8) Jasone Astorga, M. B. U. a. E. J., 2022. Revisiting the Feasibility of Public Key Cryptography in Light of IIoT Communications. *Sensors (MDPI),* p. https://doi.org/10.3390/s22072561.

9) Kosek, A., 2015. An Exploration of Mathematical Applications in Cryptography. *Thesis, The Ohio University, An Infinite Family of Perfect Parallelepipeds,* 83(289), pp. 2441-2454.

10) Mehmet Merkepci, M. A. A. A., 2023. The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm. *ASPG,* 10(2), pp. 69-74.

11) Mr. Sawant Laxman S., M. P. S. A., 2020. Cryptography and Image Processing by Matrices. *International Research Journal of Engineering and Technology (IRJET),* 7(8), pp. 4327-4330.

12) Navalakhe, R., 2021. Cryptographic Algorithms Using Finite State Machine, Bernoulli and Lucas Numbers. *South East Asian Journal of Mathematics and Mathematical Sciences,* 17(3), pp. 17-28 .

13) Navalakhe, R., 2022. Cryptography: Recent Research trends of encrypting Mathematics, Material Today. *Material Today Proceedings (Elsevier),* Volume 56, p. 3247–3253.

14) Navalakhe, R., 2023. A New Cryptography Model Using Adjoint Of Matrix. *Journal of Technology,* 11(9), pp. 43-52..

15) Navalakhe, R., 2023. Implementation of Cryptographic Algorithms using Recurrence Matrix and Moore Machine. *Punjab University Journal of Mathematics,* 55(3), pp. 89-98..

16) Pawanveer Singh, A. S. S. J., 2017. Importance of Number Theory in Cryptography. *International Journal of advance research in science and engineering,* 6(1), pp. 117-121.

17) Pizzigoni, F., 2013. Number Theory Applications in Cryptography. *Thesis, Montclair State University.*

18) Rao, M. R. a. G. S., 2017. Review on Application of Mathematics In Cryptography. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET),* 4(21), pp. 62-73.

19) Shalini Subramani, S. M. K. A. &. S. K. S., 2023. Review of Security Methods Based on Classical Cryptography and Quantum Cryptography. *Cybernetics and Systems,* p. DOI: 10.1080/01969722.2023.2166261.

20) Steven Galbraitha, A. M., 2005.. Algebraic Curves and Cryptography. *Finite Fields and Their Applications,* pp. 544-577, doi:10.1016/j.ffa.2005.05.001.

21) Waghmare Shwetambari, M. U., 2020. Development of Matrix for Cryptography. *Journal of emerging technologies and innovative research,* 7(4), pp. 112-118.

22) Yahia Alemami, M. A. M. S. A., 2019. Research on Various Cryptography Techniques. *International Journal of Recent Technology and Engineering (IJRTE),* 8(2S3), pp. 395-405.

23) Zainab Khyioon Abdalrdha, I. H. A.-Q. F. N. A., 2019. Subject Review: Key Generation in Different Cryptography Algorithm. *International Journal of Scientific Research in Science, Engineering and Technology,* 6(5), pp. 230-240.