ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

COMPARATIVE ANALYSIS OF VARIOUS ALGORITHMS FOR DATA ENCRYPTION USED IN HYBRID TECHNIQUE TO IMPLEMENTATION IN DATABASE

Satinder* and Dr. Parveen Sehgal**

* Research Scholar, Deptt. of Computer Science & Engineering , School of Engineering & Technology, Om Sterling Global University, Hisar, Haryana, India
E-Mail : satindercse192@osgu.ac.in, satindershanky@gmail.com
** Professor, Deptt. of Computer Science & Engineering , School of Engineering & Technology, Om Sterling Global University, Hisar, Haryana, India
E-Mail : drparveensehgal@osgu.ac.in, drparveensehgal@gmail.com

ABSTRACT

Data security is a top priority in today's digital world, especially when dealing with sensitive information kept in databases. Hybrid encryption systems, which integrate various encryption algorithms, have grown in popularity due to their capacity to improve data security. This study compares and contrasts several encryption methods used in hybrid database implementation strategies. The study begins with a review of data encryption foundations and then presents the notion of hybrid encryption, emphasizing its benefits in attaining strong security. Following that, a thorough examination of popular encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), and Elliptic Curve Cryptography (ECC) is performed. The comparison includes critical variables such as security strength, key size, encryption/decryption speed, resource needs, mathematical difficulty, key management, adoption/standardization, algorithm maturity, regulatory compliance, flexibility, known weaknesses, and patent/license status.

Finally, this comparison research provides significant insights into the strengths and shortcomings of various encryption algorithms in the context of hybrid strategies for database implementation.

Keywords: Security, Symmetric, Asymmetric AES, DES, Blowfish, RSA, Hybrid

INTRODUCTION

The exponential rise of information technology in today's digital era has led in an exponential increase in the volume of data created, stored, and communicated across numerous platforms. With the ever-present threat of cyber-attacks and data breaches, protecting sensitive information has become a top priority. Encryption, as one of the core data security strategies, is critical in protecting data from unauthorized access and malevolent actors. Adopting a strong encryption approach becomes essential in the context of databases, where sensitive data is frequently stored and accessed.

The goal of this research is to undertake a complete comparative examination of various encryption algorithms used in hybrid database implementation methodologies. The strengths of symmetric and asymmetric encryption systems are combined in hybrid encryption, with the goal of mitigating the flaws of each approach. Hybrid encryption tries to develop a more secure

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

and efficient encryption process by combining various approaches while maintaining a balance between encryption speed and key management complexity.

Data Encryption

Data encryption is a fundamental technology used to prevent unwanted access to sensitive information. It entails utilizing cryptographic techniques to convert plaintext data into ciphertext, leaving the data illegible without the necessary decryption key. Encryption protects the secrecy, integrity, and validity of data, making it an essential component of modern data security.

Encryptions are classified into two types: symmetric and asymmetric encryption.

Symmetric encryption uses the same secret key for both encryption and decryption. Anyone who has access to the key can decrypt the ciphertext. Because symmetric encryption is economical and quick, it is well suited for encrypting huge amounts of data. The key management procedure, on the other hand, is difficult, especially in large-scale systems.

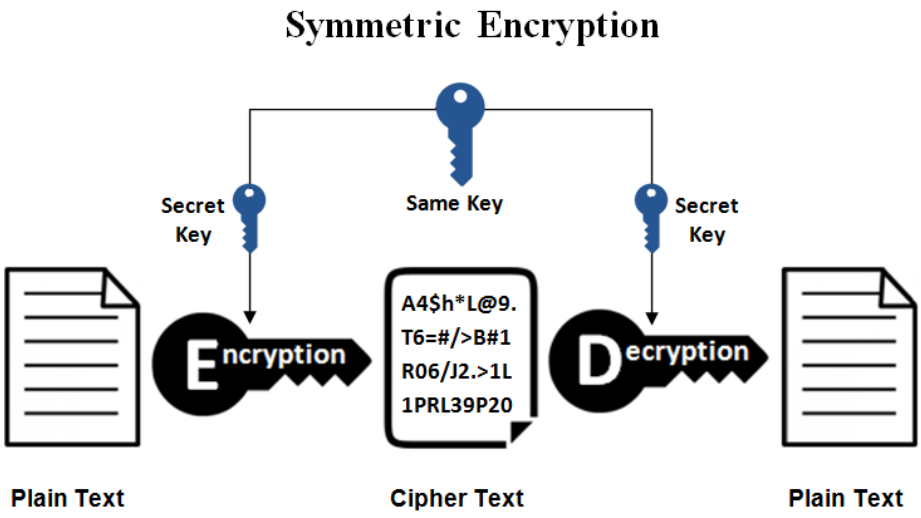

Fig. 1 Symmetric Encryption

The benefits of symmetric algorithms include faster real-time system performance compared to asymmetric algorithms. While the symmetrical algorithm's fault resides in the challenge of managing keys because it requires a unique key for every unique user. Blow Fish, DES, and AES are a few symmetric algorithms as examples.

Asymmetric encryption

A public key and a private key that are mathematically connected are used in asymmetric encryption, sometimes referred to as public-key encryption, to encrypt and decode data. While the private key must be kept secret, the public key is freely distributable. Asymmetric encryption fixes the key distribution problem while enhancing security. It is commonly used in digital signatures and key exchange.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

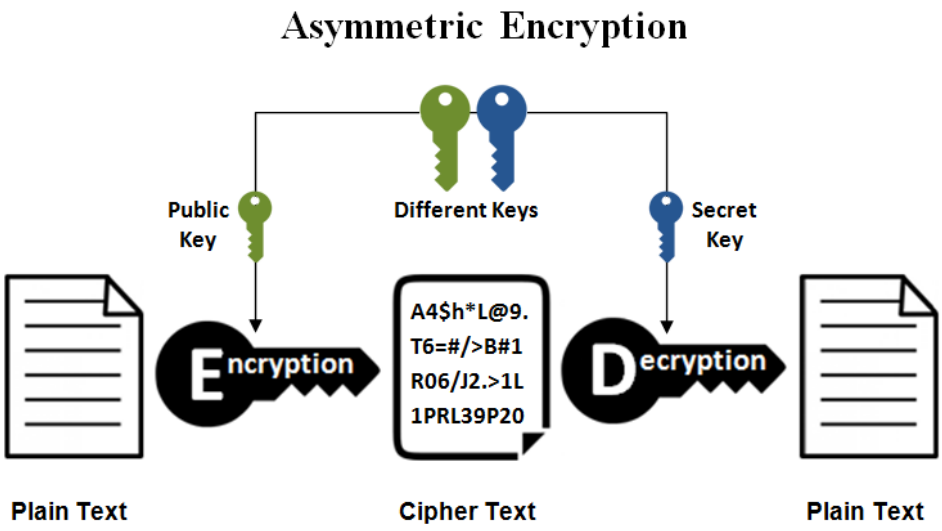

Fig. 2 Symmetric Encryption

Data is encrypted using asymmetric encryption, which ensures that only the owner of the associated private key may decrypt the data. Without the need for a shared secret key, this process enables secure data transmission and communication. When it comes to security, asymmetric algorithms have an advantage since their keys are longer than those used by symmetric algorithms and are employed differently for encryption and decryption procedures. While the asymmetric algorithm's vulnerability caused the overhead on the data packet to rise as key length rose, lowering operating speed. Asymmetric algorithms include RSA, DSA, and Diffie-Hellman, for instance.

Hybrid encryption combines the benefits of both symmetric and asymmetric encryption. It solves the shortcomings of existing technologies and provides a realistic solution to secure data transfer and storage. Asymmetric encryption is used for safe key exchange in hybrid encryption, whereas symmetric encryption is used for bulk data encryption. This method strikes a compromise between security and efficiency, making it appropriate for a wide range of applications such as secure communication, cloud computing, and database security.

Overall, data encryption is an important component of contemporary information security since it protects sensitive data from possible attacks while also maintaining privacy and secrecy in digital communication and storage.

Materials and Methods

The methodology of this study covers a number of approaches suggested to fulfill the paper's objective. Data description, the use of encryption and decryption algorithms, simulation, and an assessment of the effectiveness of the chosen algorithms are the approaches used. The study's most widely used encryption methods were AES, DES, 3DES, RSA, Diffin-Hellman, and ECC. The simulation was powered by a few chosen text data files, and the algorithms were built in a Dot Net programming environment. The effectiveness of the chosen algorithms was evaluated using metrics including encryption time, decryption time, memory use, and data size.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

ENCRYPTION ALGORITHMS

There are many types of Symmetric and Asymmetric Algorithms available as follows:

Symmetric algorithms	"AES" (Advanced Encryption Standard), "DES", "3DES", "Blowfish", "TwoFish", "ThreeFish", "RC" (Rivest Cipher) variations, "RC2, RC4, RC5, RC6, A5/1, A5/2" (mainly for GSM).
Asymmetric algorithms	"Diffie–Hellman", "Elliptic Curve", "RSA" (Rivest–Shamir–Adleman), "ElGamal" (based on Diffie–Hellman), "DSA" (Digital Signature Algorithm)

Some Strengths and Weaknesses of encryption Algorithms

Each Algorithms have their own Strengths and Weaknesses

Types of Symmetric Algorithms

Advanced Encryption Standard (AES):

Strengths:

- Proven resilience against cryptographic assaults, as well as efficient and rapid encryption and decryption operations.
- Supports key lengths of 128, 192, and 256 bits, providing for more security level flexibility.
- Widely standardized and used, guaranteeing interoperability across systems.

Weaknesses:

- Certain implementations may be vulnerable to side-channel attacks.

Triple DES (3DES) and Data Encryption Standard (DES):

Strengths:

- Historical importance as a basic encryption method. • 3DES offers more security than DES due to multiple encryption rounds and higher key lengths.

Weaknesses:

- Because DES has a tiny key length of 56 bits, it is vulnerable to brute-force assaults in current computer settings.
- When compared to newer encryption systems, 3DES is relatively sluggish and resource-intensive.

Blowfish:

Strengths:

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

- High security and resilience against cryptographic assaults.
- Efficient software implementations with competitive performance.

Weaknesses:

- Limited standardization in comparison to commonly used algorithms such as AES.

RC-6 (Rivest's Cipher 6):

Strengths:

- Designed for both hardware and software implementations, providing deployment flexibility;
- Strong security features with a flexible number of rounds and key sizes.

Weaknesses:

- Less standardization and uptake than AES.

RC4 (Rivest's Cipher 4):

Strengths:

- A simple and quick method that is appropriate for software implementation.

Weaknesses:

- Considered weak and unsecure owing to cryptographic flaws;
- No longer recommended for usage in secure applications.

Twofish:

Strengths:

- Strong security and efficiency for symmetric encryption applications;
- Supports key lengths of 128, 192, and 256 bits, allowing for security level flexibility.

Weaknesses:

- Limited standardization in comparison to commonly used algorithms such as AES.

Each encryption method has distinct features and qualities that make it appropriate for various use cases. While AES is the most extensively used and recommended symmetric encryption standard, alternative algorithms such as Blowfish and Twofish provide good security and efficiency in specific applications. DES and RC4 on the other hand are regarded weak and should be avoided in current applications. The encryption technique should be chosen after a thorough examination of the application's or system's unique security needs and performance limits.

Types of Asymmetric Algorithms

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

RSA (Rivest-Shamir-Adleman):

Strengths:

- Asymmetric encryption method based on the difficulty of factoring huge composite numbers.
- Widely used for safe key exchange, digital signatures, and secure communication.

Weaknesses:

- Computationally demanding, particularly for extended key lengths, which may result in poorer performance;
- Susceptible to quantum computing-based assaults, which may jeopardize its security in the future.

Digital Signature Algorithm (DSA):

Strengths:

- Specifically designed for digital signatures, with rapid signing and verification processes; • Strong security with suitable key lengths.

Weaknesses:

- Is restricted to digital signatures and is not suited for other types of encryption.
- Proper implementation necessitates the use of a random or pseudorandom number generator.

Diffie-Hellman (DH) Key Exchange:

Strengths:

- Provides complete forward secrecy, which means that previous conversations are safe even if private keys are compromised in the future.

Weaknesses:

- Vulnerable to man-in-the-middle attacks if not authenticated or protected with additional security procedures.
- Requires extra authentication and integrity verification processes or algorithms.

ECC (Elliptic Curve Cryptography):

Strengths:

- An asymmetric encryption technique based on elliptic curves over finite fields.
- Superior security with shorter key lengths than standard asymmetric algorithms such as RSA.
- Efficient computation and performance, which is especially beneficial in resource-constrained situations.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Weaknesses:

- Less standardized and used in outdated systems than RSA.
- Because of its recent debut, there have been less historical assessments and possibly unforeseen weaknesses.

ElGamal:

Strengths:

- Based on the Diffie-Hellman key exchange method, this asymmetric encryption algorithm provides encryption and digital signature functionality.

Weaknesses:

- Slower encryption and decryption operations when compared to symmetric encryption methods like AES.
- Key management might be difficult in some situations.

Elliptic Curve Digital Signature Algorithm (ECDSA):

Strengths:

- DSA variant that employs elliptic curve cryptography for digital signatures.
- Provides good security and efficiency while using shorter key lengths than regular DSA.

Weaknesses:

- Like DSA, ECDSA is confined to digital signatures and necessitates the use of a random or pseudorandom number generator.

Each encryption method has distinct benefits and fulfills specialized cryptographic functions. RSA is a flexible and frequently used key exchange and digital signature technology. ECC offers high security and efficiency, making it appropriate for resource-constrained situations. ElGamal combines encryption with digital signatures, whilst DH allows for safe key exchange. The algorithm used is determined by the application's or system's unique cryptography needs and performance restrictions.

COMPARATIVE ANALYSIS OF DIFFERENT CRYPTOGRAPHY ALGORITHMS

Many writers and academics have suggested various forms of comparisons for these algorithms based on different encryption techniques. In this work, we attempted to bring together all of those comparisons where we contrasted different aspects of various algorithms in the form of Key Length, Cipher Type, Block Size, Resistance, Possible Keys, Rounds, etc.

Table 1 Comparison table of various symmetric encryption algorithms

Parameter	AES	DES	3DES	Blowfish	Twofish
Security	High	Weak (Obsolete)	Moderate	Moderate	High

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Key Length	128, 192, 256	56	168	32-448	128, 192, 256
Performance	Fast	Slow	Very Slow	Fast	Fast
Industry Adoption	Widely Adopted	Historical Use	Historical Use	Limited Use	Limited Use
Cryptanalysis Research	Extensively Studied	Extensively Studied	Extensively Studied	Some Research	Some Research
Hardware Support	Hardware Support	Hardware Support	Hardware Support	No Hardware Sup.	No Hardware Sup.
Algorithm Flexibility	Limited	Limited	Limited	Flexible	Flexible
Standardization	Standardized	Standardized	Standardized	Non-standard	Non-standard
Key Management	Good	Poor	Poor	Good	Good
Block Size	128 bits	64 bits	64 bits	64 bits	128 bits
Resource Usage	Efficient	Inefficient	Very Inefficient	Efficient	Efficient
Public Scrutiny	High	Low	Low	Low	Low
Maturity	Mature	Obsolete	Mature	Mature	Mature
Vulnerability Response	Rapid	Slow	Slow	Slow	Slow
Energy Efficiency	Energy Efficient	Energy Inefficient	Energy Inefficient	Energy Efficient	Energy Efficient
Usability	User-friendly	Not User-friendly	Not User-friendly	User-friendly	User-friendly
Parallelization	Parallelizable	Not Parallelizable	Not Parallelizable	Parallelizable	Parallelizable
Resistance to Attacks	Strong	Vulnerable	Resistant to Attacks	Vulnerable	Resistant to Attacks
Mode of Operation	Various Modes	ECB and CBC	ECB and CBC	Various Modes	Various Modes

Table 2 Comparison table of various asymmetric encryption algorithms.

Parameter	**RSA**	**DSA**	**Diffie-Hellman (DH)**	**ECC**	**ElGamal**
Security	High	High	High	High	High
Key Length (bits)	2048+	1024+	2048+	256+	2048+

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Performance	Moderate	Efficient	Efficient	Efficient	Slower
Industry Adoption	Widespread	Limited	Limited	Less Standardized	N/A
Cryptanalysis Research	Extensive	Limited	Limited	Limited	N/A
Hardware Support	Widely supported	Moderate	Moderate	Moderate	N/A
Algorithm Flexibility	Moderate	Limited	Key Exchange	Limited	Key Exchange
Standardization	Widely Adopted	Standardized	N/A	Limited	N/A
Key Management	Moderate	Moderate	Moderate	Moderate	Moderate
Block Size	N/A	N/A	N/A	N/A	N/A
Resource Usage	High	Low	Low	Low	Moderate
Public Scrutiny	High	High	High	High	High
Maturity	Mature	Mature	Mature	Mature	Mature
Vulnerability Response	Prompt	Prompt	Prompt	Prompt	Prompt
Energy Efficiency	Moderate	High	High	High	High
Usability	Moderate	High	High	High	High
Parallelization	Limited	High	High	High	High

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Resistance to Attacks	Vulnerable to Quantum	No Quantum Attack	Vulnerable to MITM	Potential Unknown	N/A
Mode of Operation	N/A	N/A	N/A	N/A	N/A

In this section, several parameters are used to compare the performance of a few key symmetric cryptographic algorithms (Blow Fish, DES, AES) and asymmetric keys (RSA, DSA, and Diffie-Hellman). Key types employed, security level, key size, speed of encryption and decryption, resource requirements, mathematical challenge, key management, adoption/standardization, algorithm maturity, regulatory compliance, adaptability, known flaws, and patent/license status are among the parameters examined. Table 3 might be used to display the findings of the literature synthesis for both symmetric and asymmetric key methods.

Table 3 The synthesis process results of Symmetric and asymmetric key algorithms

Parameter	AES	DES	Blowfish	RSA	Diffie-Hellman (DH)	ECC
Security	High	Weak (Obsolete)	Moderate	High	High	High
Key Length	128, 192, 256	56	32-448	2048+	2048+	256+
Performance	Fast	Slow	Fast	Moderate	Efficient	Efficient
Industry Adoption	Widely Adopted	Historical Use	Limited Use	Widespread	Limited	Less Standardized
Cryptanalysis Research	Extensively Studied	Extensively Studied	Some Research	Extensive	Limited	Limited
Hardware Support	Hardware Support	Hardware Support	No Hardware Sup.	Widely supported	Moderate	Moderate
Algorithm Flexibility	Limited	Limited	Flexible	Moderate	Key Exchange	Limited
Standardization	Standardized	Standardized	Non-standard	Widely Adopted	N/A	Limited

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Key Management	Good	Poor	Good	Moderate	Moderate	Moderate
Block Size	128 bits	64 bits	64 bits	N/A	N/A	N/A
Resource Usage	Efficient	Inefficient	Efficient	High	Low	Low
Public Scrutiny	High	Low	Low	High	High	High
Maturity	Mature	Obsolete	Mature	Mature	Mature	Mature
Vulnerability Response	Rapid	Slow	Slow	Prompt	Prompt	Prompt
Energy Efficiency	Energy Efficient	Energy Inefficient	Energy Efficient	Moderate	High	High
Usability	User-friendly	Not User-friendly	User-friendly	Moderate	High	High
Parallelization	Parallelizable	Not Parallelizable	Parallelizable	Limited	High	High
Resistance to Attacks	Strong	Vulnerable	Vulnerable	Vulnerable to Quantum	Vulnerable to MITM	Potential Unknown
Mode of Operation	Various Modes	ECB and CBC	Various Modes	N/A	N/A	N/A

FINDINGS AND DISCUSSION

In this section, asymmetric keys and different key symmetric cryptography techniques are discussed from multiple linked topics, including:

A widely used cryptographic technique is presented in research [1] and may be divided into two categories: symmetrical and asymmetrical techniques. Analysis of two different types of cryptographic methods from the perspectives of data security and computational complexity reveals that both are equally accurate, but the asymmetric method has more complexity and a longer processing time. However, both asymmetric methods have a higher level of data security.

A comparison of studies between several encryption algorithms, including AES, DES, RSA, and DIFFIE-HELLMAN, is shown in research [2] by contrasting the many aspects of both symmetric keys and asymmetric key encryption methods. When the results of the encryption technique were studied in terms of symmetric lock and asymmetric key algorithm, it was found that symmetric key algorithm was better in terms of speed and power consumption than asymmetric key algorithm was.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

How much security the route offers when transporting data is the fundamental aspect of internet security, according to research [3]. One method for enabling secure data transport without compromising integrity and secrecy is cryptography technology. The two fundamental categories of cryptography—symmetric key cryptography and asymmetric key cryptography—are based on key distributions. The suggested approach is shown to be highly efficient when compared to the significance of these two cryptographic techniques, however there are still certain issues that are connected to this algorithm that have not been fully resolved. The article also offers a suitable outlook for this untapped subject in the future.

The overview of asymmetric key algorithms in research [4] covers the history of asymmetric cryptography from its inception in 1976 to the present. This page describes how each method performs encryption and decryption, highlighting its fundamental security, area of use, and operational benefits and drawbacks. Based on the findings of the research, the journal also identifies a gap that still needs to be filled, with a focus on algorithms that are most appropriate for the application industry in light of recent developments.

Research [5] assesses the effectiveness of cryptographic algorithms to determine the best algorithms to utilize moving forward. This study contrasts symmetric (AES, DES, Blowfish) and asymmetric (RSA) algorithms with various file formats, including binary, text, and picture files. Evaluation criteria like throughput for decryption and encryption time have been compared. To illustrate how well each method works, simulation results are provided.

Research [6] investigated a few symmetric key cryptography-based suggested procedures and created a comparison research framework. This article describes the fundamental characteristics, benefits, drawbacks, and applications of several symmetric key cryptography algorithms.

Research [7] focuses on the private key blocks of ciphers often used for bulk data and encryption connections and gives peer analysis in the area of encryption methods. A comparison of a few well-known and effective algorithms was also done in this work. The comparative analysis of all encryption methods is a secondary subject of this literature review. the rationale of experimental study. This article also discusses the performance metrics used to analyze security vulnerabilities and carry out the encryption procedure.

CONCLUSION

We have made an effort to compare the majority of the encryption algorithms in use with the various types of parameters provided by various authors and researchers. According to the table in the previous section, symmetric and asymmetric keys both have benefits and drawbacks when used with the synthesized data. Comparative measuring factors, such as callability, accuracy, convenience of use, and others, might be introduced as additional study recommendations. In order to make comparisons between different cryptographic algorithms that employ symmetric and asymmetric keys easier and more precise, further research can also use the framework for measuring variables. Additionally, the outcomes illustrated the traits of the chosen algorithms (RSA, AES, and DES) in terms of metrics taken into account in the study, providing additional clarity on the application of the different cryptographic algorithms. The

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

study's findings are pertinent and will help users and designers select the best cryptographic algorithms for a given application's security requirements.

References

[1.] Devi, A., Sharma, A., & Rangra, A. (2015). A Review on DES, AES and Blowfish for Image Encryption & Decryption. IJCSIT Int J Comput Sci Inf Technol 6(3):3034–3036.

[2.] Bala, M,. Kumari, P., & Sharma, A. (2017) Comparative analysis of symmetric key algorithms: DES, AES and blowfish for audio encryption and decryption. IEEE, pp 1048–1054.

[3.] Jeeva, A. L., Palanisamy D. V., & Kanagaram K (2012) Comparative analysis of performance efficiency and security measures of some encryption algorithms. Int J Eng Res Appl 2 (3):2248–9622.

[4.] Tamimi A.A. (2008) Performance analysis of data encryption algorithms. IEEE retrieved Oct vol 1, pp 399–403.

[5.] Kumar Y., & Munjal R, (2011) Comparison of symmetric and asymmetric cryptography with existing vulnerabilities, IJCMS.

[6.] Mehlrotra S, Seth, & Mishra R, (2011) Comparative Analysis of Encryption Algorithms For Data Communication, IJCST Vol. 2, Issue 2.

[7.] Kumar, A.Y. (2013) Comparative Study of Different Symmetric Key. International Journal of Application or Innovation in Engineering & Management , 2, 204-206.

[8.] Karule, K.P. & Nagrale, N.V. (2016) Comparative Analysis of Encryption Algorithms for Various Types of Data Files for Data Security. International Journal of Scientific Engineering and Applied Science , 2, 495-498.

[9.] Pavithra, S. & Ramadevi, E. (2012) Study and Performance Analysis of Cryptography Algorithms. International Journal of Advanced Research in Computer Engineering & Technology, 1, 84.

[10.] Mathur, M. & Kesarwani, A. (2013) Comparison between DES, 3DES, RC2, RC6, Blowfish and AES. Proceedings of National Conference on New Horizons in IT, NCNHIT , Mumbai, September 2013, 143-148.

[11.] Bala, T. & Kumar, Y. (2015) Asymmetric Algorithms and Symmetric Algorithms: A Review. Proceedings on International Conference on Advancements in Engi neering and Technology ICAET, August 2015, 1-4.

[12.] Verma, A., Guha, P. & Mishra, S. (2016) Comparative Study of Different Cryptographic Algorithms. International Journal of Emerging Trends & Technology in Computer Science , 5, 58-63.

[13.] Bisht, N. & Singh, S., (2015) A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms International Journal of Innovative Research in Science, Engineering and Technology4, 3 p. 1028–1031.

[14.] Tripathi, R. & Agrawal, S., 2014, Comparative Study of Symmetric and Asymmetric Cryptography Techniques, International Journal of Advanced Foundation and Research in Computer1, 6 p. 68–76.