Application of Advanced Encryption Standard (AES) for Securing Electronic Banking Transactional Data

[*]Abubakar Zubairu Muazu[1], Bala Modi[2], Mohammed Usman[3], M.K Ahmed[4]

[1, 2,4]Department of Computer Science, Gombe State University, Gombe, Nigeria

[3]Department of Computer Science, Modibbo Adama University, Yola, Nigeria

[*]Corresponding Author

DOI: https://doi.org/10.51584/IJRIAS.2025.100800074

Received: 09 August 2025; Accepted: 16 August 2025; Published: 12 September 2025

ABSTRACT

Due to the rapid growth and convenience of electronic payments, many customers are opting for e-banking platforms to complete their transactions with ease. However, the rise in cyber threats to e-banking transactional data poses numerous risks to both banks and customers. This research addresses the pressing need for enhanced security measures amidst rising cyber threatss in electronic banking transactions by evaluating the performance and effectiveness of the Advanced Encryption Standard in comparison with Blowfish, RSA and ECC Algorithms. It assessed the Encryption/Decryption speed and throughput using Python Programming Language to secure large transactional datasets ensuring safer e-banking Data Storage for Banks. Recommendations are also provided for further enhancing the security of e-banking transactional data.

Keywords: Cyber Threat, e-banking, Transaction, Advanced Encryption Standard (AES), RSA, Blowfish, Elliptic Curve Cryptography (ECC)

INTRODUCTION

The landscape of financial transactions has undergone a rapid and transformative shift towards digital platforms. While this transition has brought unprecedented convenience and accessibility, it has also brought to the forefront, the critical issue of transaction security. As financial activities increasingly migrate to online environments, concerns about the vulnerability of these transactions to cyber threatss have escalated. (Shazmeen & Prasad, 2021).

Vishnupriya & Rao, (2024) also stated that the rapid growth of online platforms has expanded the attack surface for cybercriminals, exposing sensitive financial data and transactions to potential breaches. The evolving nature of cyber threatss necessitates a proactive and multi-faceted approach to fortify transaction security, ensuring the confidentiality, integrity, and authenticity of financial interactions.

Cryptographic methods offer a robust framework for protecting data throughout its lifecycle – from origination and transmission to storage. By employing established cryptographic algorithms, financial institutions can effectively safeguard the confidentiality of sensitive information, mitigating the risk of unauthorized access. (Aziz, Rodiah, & Susanto, 2021).

Symmetric vs Asymmetric Cryptography

Encryption is an important tool for keeping information private and safe. Only users with the right key can unlock and read the encrypted data. In cryptography, the main goal is to stop unauthorized people from accessing information. Data in its original, readable form is called plaintext, while unreadable data is called ciphertext. The process of turning plaintext into ciphertext is called encryption, and it helps ensure data security. (Afolabi, & Atanda, 2016).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

Figure 1 illustrates the classification of Cryptography. The encryption algorithms are basically classified into symmetric and asymmetric algorithms due to the way they function. Symmetric algorithms use the same key for encryption and decryption of data. The key is securely concealed and transmitted to the intended receiver, often protected by an additional key. This extra layer of security is necessary because if the key is intercepted, the message can be easily compromised. (Abood, & Guirguis, 2018).

The algorithms are further divided into stream ciphers and block ciphers. Stream ciphers encrypt data one bit at a time, while block ciphers encrypt groups of bits together. Block ciphers use an initialization vector to avoid producing the same ciphertext for repeated data. This added randomness strengthens security. As a result, block ciphers are more effective for encrypting large amounts of data than stream ciphers. (Omijeh & Agughalam, 2020).

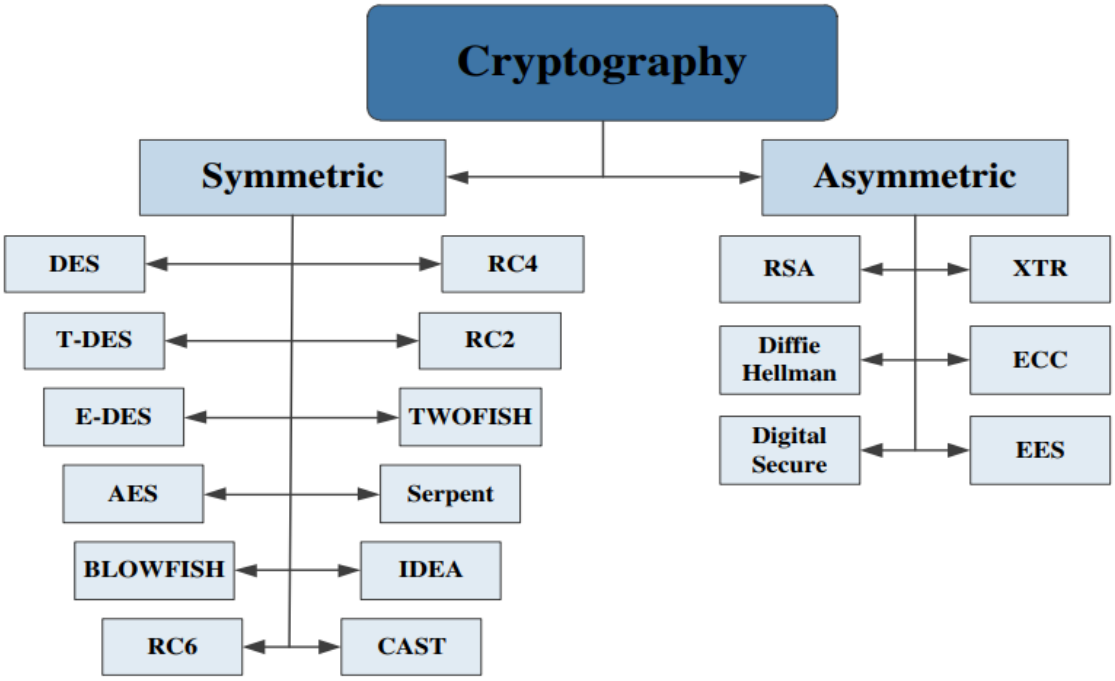

Figure 1: Classification of Cryptography (Source: Abood, & Guirguis, 2018).

This research explores cryptographic techniques to show their practical importance in improving transaction security, with a focus on the Advanced Encryption Standard (AES) algorithm. By examining related datasets and challenges, the study aims to give useful insights on how cryptographic methods can be applied in Nigerian financial institutions.

STATEMENT OF PROBLEM

The increasing reliance on e-banking transactions pose significant security challenges, with potential vulnerabilities that expose customers and banks to various cybersecurity threats, including fraud, identity theft, and data breaches. (Omijeh & Agughalam, 2020).

While encryption technologies such as Advanced Encryption Standard (AES) offer robust security measures, their effective application in securing e-banking transactional data remains underexplored, particularly in the context of most of the works reviewed.

LITERATURE REVIEW

A variety of scholarly articles addressing Cyber threats and fraud prevention in banking transactions were examined, ranging from those focused on non-cryptographic solutions to those employing Cryptographic

solutions to mitigate and secure transactions from unauthorized access. The findings clearly indicate that the advantages of Cryptography extend to banks, customers, and society as a whole.

Abood & Guirguis, (2018), worked on the performance comparison of AES with other algorithms like DES, TDES, DSA, RSA, ECC, Blowfish etc. in terms of speed, encryption time and flexibility. It was concluded that AES was the best and most efficient compared to the others in terms of security, flexibility and encryption performance.

Agbelusi & Olumuyiwa, (2023), compared AES and RSA in terms of the performance of encryption and decryption time. The result showed that AES was the best between the two algorithms. The author recommended AES as the better algorithm for data security especially in Banking systems.

Al-Shabi, (2019), compared the performance of some symmetric and asymmetric algorithms and concluded that AES was more reliable in terms of encryption and decryption speed and usability.

Amaka, Eneh, Udanor & Nduka, (2019) worked on the implementation and adoption of e-banking transactions in Nigeria and suggested that for it to gain more acceptance and popularity amongst its users, there is a growing need for optimum security of the e-banking system at large.

Assa-Agyei & Olajide, (2023) compared AES with Blowfish and Twofish algorithms in terms processing time (throughput) with consistent key size of 128 bits and concluded that AES was the best for securing data.

Buhari, Obiniyi, Sunday & Shehu, (2019) conducted research on the performance of AES and Blowfish algorithms based on execution time and throughput on different types of data. The results showed that for small data size, Blowfish was faster in terms of execution time and AES was better in terms of throughput. The use of large data was recommended to calculate the performance in terms of execution time and throughput.

Komal, Kumar, Kumar, Kashyap & Rana, (2023) compared AES, DES, RSA and ECC in terms of execution time and CPU speed performance. The result showed that AES provided better security in terms of performance analysis. Also recommended AES for future work.

Hamouda, (2020) worked on the performance of DES, 3DES and AES in terms of encryption time and throughput. The results showed that AES was best in terms of security. Also recommended AES for securing different types of data in future research.

Research Gap

A variety of scholarly articles addressing the use of Cryptography for securing data were examined as seen previously in the review of related literature, were most of the studies focused on encrypting different types of data ranging from text files, audio files, video files to mobile banking transaction end to end encryption to secure them from unauthorized access. There is not much on transactional database encryption.

This research work in contrast to the reviewed is concerned with the encryption of e-banking transaction datasets. It focused on large datasets to examine the strengths of the AES algorithm in terms of encrypting large amounts of data due to the large customer base of deposit money Banks to enable the encryption of the customer information in the database.

METHODOLOGY

This research aims at investigating the performance of the Advanced Encryption Standard (AES) in securing e-banking transactional data. The methodology encompasses several key stages: data collection, data pre-processing, encryption and decryption using AES, Blowfish, RSA and ECC. Performance evaluation using speed and throughput and comparison of the results. Each stage is designed to ensure that the data is handled securely and that the performance of AES is assessed accurately and comprehensively.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

In this work, AES, Blowfish, RSA and ECC encryption algorithms have been implemented in Python Programming Language and the experiment has been carried out using a laptop having Intel(R) Core (TM) i5 @ 2.60GHz processor with 8 GB RAM on Windows 11 Enterprise, 64-bit operating system. The experiment program was compiled using the Sublime Text code editor. The experiment was performed couple of times to assure that the results are consistent and are valid to compare the different algorithms.

Transactional Data from the Banks and Synthetic Data

Some of the Transactional Data collected include:

Sender/Receiver Account information

Transaction Amount

Transaction Fees

Transaction ID

Time Stamp

Data pre-processing

The data undergoes pre-processing steps below before encryption and decryption.

Data Cleaning: Ensure that there are no duplicates or erroneous records in the dataset.

Normalization: Normalize transaction amounts and timestamps to ensure consistency.

Categorical Encoding: Convert categorical variables (e.g., Transaction Type) into numerical format to facilitate the encryption and classification process.

AES Encryption and Decryption

As illustrated in Figure 2, the encryption and decryption process flow chart are depicted. The key size variation determines the AES encryption-decryption process: 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. A 4×4-byte matrix is used in each round to process data which is known as “the state” and series of transformations are applied -SubBytes, ShiftRows, MixColumns, and AddRoundKey - to progressively conceal the plaintext. The final round skips the MixColumns step to produce the ciphertext. This structured, multi-round approach is what gives AES its high security and efficiency, making it well-suited for securing large-scale E-Banking transactional data. Decryption follows the reverse order, applying the inverse of each transformation to retrieve the original. (Abood, & Guirguis, 2018).

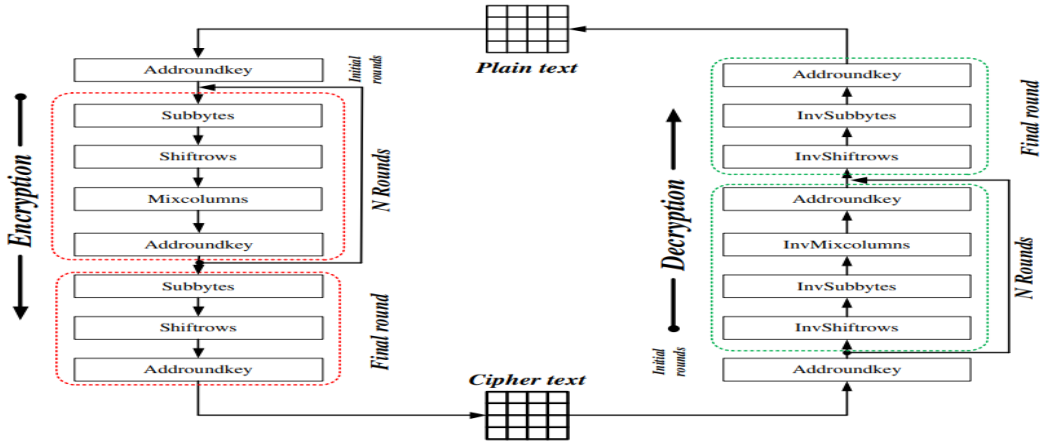

Figure 2: Flow chat of encryption and decryption of AES Algorithm (Source: Abood, & Guirguis, 2018).

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

Blowfish Encryption and Decryption

Figure 3 depicts the Blowfish encryption and decryption process built around a 16-round Feistel network. A key-dependent permutation and a key- and data-dependent substitution are applied in each round using precomputed S-boxes., Blowfish performs key expansion before any encryption begins, converting keys of up to 448 bits into several subkey arrays totalling 4,168 bytes. It generates P-array and S-boxes in this step which are critical for both encryption and decryption. Unlike AES, Blowfish's performance depends heavily on the precomputation stage, which can make initial setup slower but allows for fast encryption of subsequent data blocks (Commey, Klogo & Gadze, 2020).

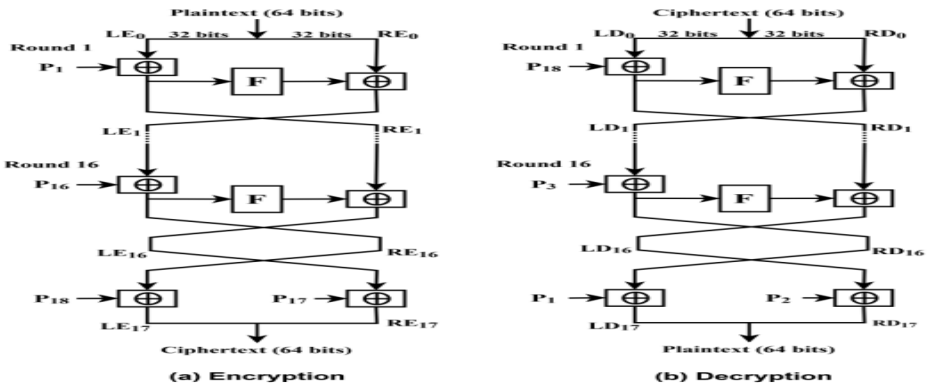

Figure 3: Flow chat Blowfish Encryption and Decryption (Source: Commey, Klogo & Gadze, 2020).

RSA Encryption and Decryption

Commey, Klogo, & Gadze, (2020) stated that RSA is the most popular asymmetric or public key cryptography that works on the concept of dual keys. The public key of the sender is utilized for encrypting the text whereas a secret key is utilized for decryption. This is an adaptable and universally used algorithm that depends upon prime factorization and considers large prime numbers for security.

Figure 4 outlines the RSA algorithm's key generation and encryption-decryption stages. The figure shows how two large prime numbers are chosen and multiplied to form the modulus, from which the quotient and key pairs are derived. Encryption involves raising the plaintext to the power of e modulo n, while decryption applies the private exponent d. The security of RSA lies in the difficulty of factoring large numbers, but its computational intensity makes it slower than AES or Blowfish for large datasets — a factor relevant when comparing algorithm suitability for e-banking systems

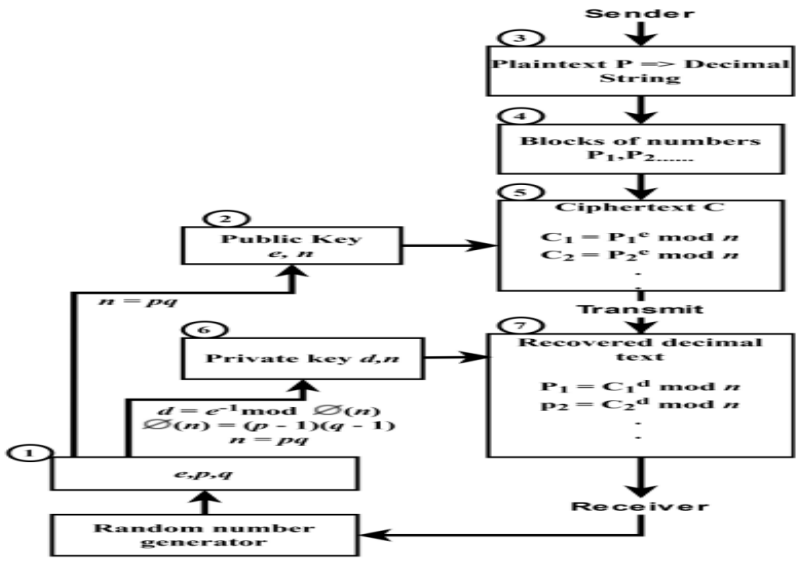

Figure 4: Flow chat RSA Encryption and Decryption (Source: Commey, Klogo & Gadze, 2020).

ECC Encryption and Decryption

The principle of Elliptic Curve Cryptography (ECC) is depicted in Figure 5, which relies on the algebraic structure of elliptic curves over finite fields. In the example shown, adding two points P and Q on the curve yields a third point R — a process known as point addition. ECC uses this mathematical property to generate public-private key pairs and perform encryption and decryption operations with relatively small key sizes compared to RSA. This results in lower computational requirements and faster processing, which can be advantageous in mobile or resource-constrained e-banking environments (Al-Shabi, 2019).

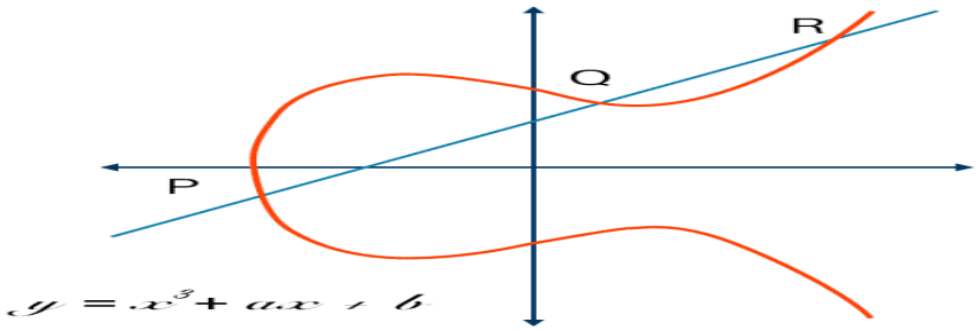

Figure 5: Elliptic Curves (Source: Komal, Kumar, Kumar, Kashyap & Rana, 2023).

Architectural Differences Between AES, Blowfish, RSA, and ECC

The performance differences observed in this study can be directly linked to the fundamental architectural characteristics of each algorithm:

AES is a symmetric block cipher that processes fixed 128-bit blocks with key sizes of 128, 192, or 256 bits. It operates through multiple substitution–permutation rounds, which makes it fast for bulk data encryption (Abood, & Guirguis, 2018).

Blowfish is also a symmetric block cipher, using a Feistel network structure with 64-bit block size and variable key length (up to 448 bits). While efficient for smaller data, its smaller block size and more complex key schedule can make it slower for large datasets (Commey, Klogo & Gadze, 2020).

RSA is an asymmetric cryptosystem based on the difficulty of factoring large integers. It uses a pair of public and private keys, making it slower due to intensive mathematical operations. It is better suited for encrypting small amounts of data, such as keys, rather than bulk data (Commey, Klogo & Gadze, 2020).

ECC is another asymmetric algorithm, based on the mathematics of elliptic curves. It provides equivalent security to RSA with smaller key sizes, but still involves higher computational cost compared to symmetric ciphers (Al-Shabi, 2019).

It is concluded from above that symmetric algorithms (AES, Blowfish) are inherently faster for bulk data encryption than asymmetric algorithms (RSA, ECC), and block size also plays a role in throughput and speed.

Performance Evaluation

To assess the performance of the proposed AES encryption and decryption, Speed and throughput were used as the performance metrics.

Speed

The time taken to convert plaintext into ciphertext and to convert ciphertext back to plaintext determines the speed for the encryption and decryption respectively. It is measured in seconds (or milliseconds). The faster the encryption, the more efficient the algorithm is, especially for real-time or high-volume data.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

Throughput

The amounts of data that can be processed (encrypted or decrypted) per unit time, typically measured in Mbps (megabits per second) or similar units. Higher throughput indicates faster overall processing, meaning more data can be securely handled in less time.

throughput = Data processed/Time

RESULTS AND DISCUSSION

Table 1 shows the datasets from the banks and synthetic e-banking transaction records generated from python's "Scikit" and "panda" libraries were used for the research. The datasets contain 20000 transactional data with the following attributes.

Transaction ID: A unique identifier for each transaction.

Time Stamp: The date and time when the transaction was initiated.

Transaction Amount: The monetary value of the transaction.

Transaction Type: Indicates whether the transaction is a 'Credit' or 'Debit'.

Transaction Status: A label indicating whether the transaction is 'Secure' or 'Insecure'.

Table 1: Sub Set of e-banking Transactional Data

Transaction ID	Time Stamp	Transaction Amount	Transaction Type	Transaction Status
1	20:17	2485.48	Credit	Failed
2	24:17	2204.04	Debit	Completed
3	01:12	4000.00	Debit	Completed
4	12.00	1000.00	Debit	Completed

Encryption and Decryption

Encryption process:

AES, Blowfish, RSA and ECC algorithms are applied to encrypt sensitive fields in the dataset. The following steps outline the encryption process:

Key Generation: Encryption key is generated.

Data Encryption: Fields such as Transaction ID and Transaction Amount are encrypted, converting plaintext into ciphertext.

Decryption process:

Decryption is the reverse of encryption, involving:

Key Retrieval: The encryption key is retrieved securely.

Data Decryption: The algorithms change the ciphertext back into plaintext, making it possible to check and confirm the original data.

Table 2 below shows encrypted and decrypted Transaction ID which is a sub set of the dataset.

Table 2: Sub Set of Encrypted and Decrypted data

Original Transaction ID	Encrypted Transaction ID	Decrypted Transaction ID
1	Q2Fz5ZZ6zGpSjfls5PAmgQ==	1

Experimental Results

To determine the speed and throughput, AES, ECC, RSA and Blowfish Cryptographic algorithms were implemented in Python programming language on 20000 transactional data. The experimental results are indicated using tables and figures. The time taken to encrypt and decrypt dataset is given in milliseconds (ms), while throughput was calculated in megabytes per second

Performance Comparison of Algorithms

Speed (Time) Comparison

Table 3: Speed (Time) Results

	Encryption Time(ms)	Decryption Time(ms)
AES	850.84	46.97
RSA	21,077.72	135,392.91
BLOWFISH	927.00	62.95
ECC	7,455.49	31,793.51

The above table 3 shows the data values of results of encryption, decryption time obtained using AES, RSA, Blowfish and ECC Algorithms. The encryption and decryption time are captured and recorded in milliseconds (ms)

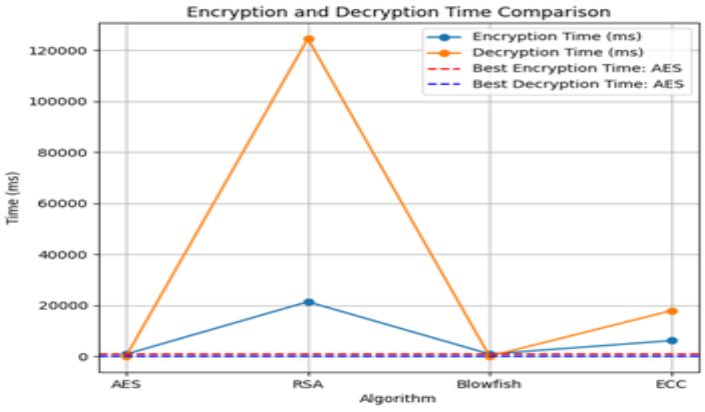

Figure 6: Encryption/Decryption Speed Comparison Graph

In figure 6 above, the dotted red line shows that AES has the lowest encryption time. The yellow straight line shows that RSA has the highest encryption time. The dotted blue line shows that AES has the lowest decryption time. The blue straight line shows that RSA also has the highest decryption time. In conclusion, it is clear from the graph that AES algorithm has the lowest encryption and decryption time which means it's the best among the four algorithms in terms of encryption and decryption speed.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

Throughput Comparison

Table 4: throughput Results

	Encryption throughput (MB/s)	Decryption throughput (MB/s)
AES	81.75	1,481.69
RSA	3.30	0.51
BLOWFISH	75.11	1,104.71
ECC	9.33	2.19

The above table 4 shows the data values of results of encryption, decryption throughput obtained using AES, RSA, Blowfish and ECC Algorithms. The encryption and decryption throughput are captured and recorded in milliseconds (MB/s).

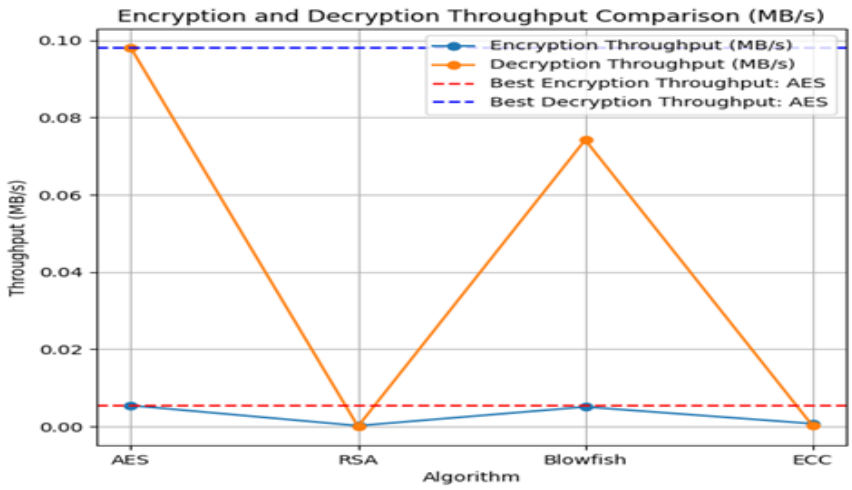

Figure 7: Encryption/Decryption throughput Comparison Graph

In figure 7 above, the dotted red line shows that AES has the highest encryption throughput. The yellow straight line shows that RSA has the lowest encryption throughput. The dotted blue line sows that AES has the highest decryption throughput. The blue straight line shows that RSA also has the lowest decryption throughput. In conclusion, it is clear from the graph that AES algorithm has the highest encryption and decryption throughput which means it's the best among the four algorithms in terms of encryption decryption throughput.

DISCUSSION OF RESULTS

Based on the performance results provided from the experiment in the research, AES (Advanced Encryption Standard) outperforms the other algorithms in all key performance metrics: encryption time, decryption time, encryption throughput, and decryption throughput.

AES has the shortest encryption/decryption time compared to RSA, Blowfish, and ECC. This means AES encrypts data faster, which is crucial for large number of datasets. RSA takes significantly longer to encrypt data, making it less suitable for the process.

AES has the highest encryption/decryption throughput, meaning it can process and encrypt more data per second compared to the other algorithms. This high throughput indicates that AES is more efficient in handling large volumes of data, which is advantageous for encrypting large datasets quickly.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue VII July 2025

In conclusion: From the experiment in the research, AES is superior to RSA, Blowfish, and ECC for encrypting large datasets in this comparison due to its:

Faster Encryption and Decryption Time: AES completes both encryption and decryption significantly quicker.

Higher throughput: AES can process and handle more data per second, making it more efficient for high-volume applications.

RECOMMENDATION

Based on the analysis conducted, it is recommended that financial institutions, particularly those involved in e-banking services, prioritize the implementation of AES for securing digital transactional data in their database. The study's comparative analysis suggests that AES outperforms other algorithms in terms of both speed and throughput, making it an ideal choice for environments requiring high-performance encryption of large amounts of data.

CONCLUSION

In conclusion, this study has demonstrated that AES is a highly effective encryption standard for securing e-banking transactions, outperforming other cryptographic algorithms in key performance metrics. The research underscores the importance of selecting the right encryption algorithm to ensure the confidentiality, integrity, and availability of sensitive financial data.

REFERENCES

1. Abood, O., Guirguis, S., (2018). A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications, 8(7), 495.
2. Afolabi, A. O., & Atanda, O. (2016). Comparative Analysis of Some Selected Cryptographic Algorithms. Computing, Information Systems, Development Informatics & Allied Research Journal, 41–52. https://www.researchgate.net/publication/306425963
3. Agbelusi, O., & Olumuyiwa, M. (2023). Comparative Analysis of Encryption Algorithms. European Journal of Technology, 1, 1–9. https://www.ajpojournals.org
4. Al-Shabi, M. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. International Journal of Scientific and Research Publications, 9(3), p8779. https://doi.org/10.29322/ijsrp.9.03.2019.p8779
5. Amaka, C., Eneh, A., Udanor, C., MO, O., & Nduka, U. (2019). Determining the adoption of e-transaction authentication frameworks in Nigerian Commercial Banks. International Journal of Engineering and Technology, 11(6), 1108–1115.
6. Assa-Agyei, K., Olajide, F., (2023). A Comparative Study of Twofish, Blowfish, and Advanced Encryption Standard for Secured Data Transmission. In IJACSA) International Journal of Advanced Computer Science and Applications: Vol. Vol. 14 (Issue No. 3, pp. 393–394). https://thesai.org/Downloads/Volume14No3/Paper_44-
7. Aziz, N., Rodiah, R., & Susanto, H. (2021). Encrypting of Digital Banking Transaction Records: A Block Chain Cryptography Security Approach. In International Journal of Computer Applications (pp. 21–22).
8. Buhari, B. A., Obiniyi, A. A., Sunday, K., & Shehu, S. (2019). Performance Evaluation of
9. Symmetric Data Encryption Algorithms: AES and Blowfish. Saudi Journal of Engineering and Technology, 04(10), 407–414.
10. Commey, D., Klogo, S. G., & Gadze, J. D. (2020). Performance comparison of 3DES, AES,
11. Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. In International Journal of Computer Applications (pp. 17–18).
12. Hamouda, B. H. (2020). Comparative Study of Different Cryptographic Algorithms.
13. Journal of Information Security, 11(03), 138–148. https://doi.org/10.4236/jis.2020.113009
14. Komal, Kumar, N., Kumar, S., Kashyap, A. K., Rana, R. (2023). Performance Evaluation of Cryptography Algorithms: AES, DES, RSA, and ECC. In Journal of Emerging Technologies and Innovative Research (Vol. 10, Issue 1) [Journal-article]. https://www.jetir.org

15. Omijeh, B. O., Agughalam, D. M., (2020). Simulation-Based Comparative Analysis of Cryptographic Algorithms. In Uniport Journal of Engineering & Scientific Research (Vol. 5, Issue Special Issue, pp. 1–10).
16. Shazmeen, S. F., & Prasad, S. (2021). A Practical Approach for Secure Internet Banking based on Cryptography. In International Journal of Scientific and Research Publications (Vol. 2, Issue 12, p. 1). https://www.ijsrp.org
17. Vishnupriya, N., P, T., & Rao, P. B. (2024). A Study On Cyber Security Issues Affecting Online Banking and Transactions. International Journal of Advance Research and Innovative Ideas in Education, 9–9(6), 1655–1656. https://www.researchgate.net/publication/378869599