Intelligent Block Ciphering System with Dynamic Key Length

Ayad Osama Jalal[١], Mazin Haithem Razuky[٢]

[١]Faculty of Administration and Economics, Al-Iraqia University, Baghdad, Iraq

[٢]University of Information Technology and communications, Baghdad, Iraq

[١]ayad.o.jalal@aliraqia.edu.iq ,[٢] dr.mazin_haithem@uoitc.edu.iq

Abstract

As long as we are trapped within the services of the electronic environment and its facilities (sending and Receiving Files), the electronic environment and its contents may be exposed to attacks by unauthorized persons to achieve the goals of data theft and sabotage and complete sending (after it has been sabotaged) to the recipient, so the files must be preserved and given a warning that the contents of the sent files have been tampered with by sending a sensor message to the sender and recipient about the status of the file. The file is encrypted with a variable-length key to prevent external attacks. After implementing the proposed system, results showed up to a ٩١٪ improvement in performance compared to traditional (non-intelligent) encryption methods.".

Key words: Intelligent Block cipher, Dynamic key length, Cryptography, ٣DES, Transposition cipher

١. Introduction

The world has witnessed a massive technological revolution in recent decades[١], leading to the emergence of what is known as the “electronic environment”[٢],[٣], characterized by rapid advancements in technology that have significantly altered how we live and interact through digital communication, online platforms, and the integration of technology into everyday activities and processes[٤].Data security is a paramount issue within the digital domain, as numerous hackers constantly seek to exploit vulnerabilities, destroy sensitive data, and blackmail organizations for financial gain. Protecting this information is essential to maintain trust and operational integrity [٥],[٦].

This paper is organized as follows: Section ٢ delves into block ciphers and associated techniques. The proposed system for this research was presented in section ٣. Section ٤ reviews the experimental result and finally, section ٥ dealt

with the most prominent conclusions that were recorded through the application of the proposed system.

٢. Block Cipher and Techniques

There are two types of symmetric key encryption: block ciphers and stream ciphers [٧],[٨]. Stream ciphers enable the encryption and decryption of data streams using a symmetric key method [٩]. In contrast, Block ciphers handle data one block at a time by dividing the plaintext or message into blocks, with each block processed separately using a key and a cryptographic algorithm [١٠]. Block ciphers successfully process information through segmenting it right into specific-sized blocks, usually ٦٤ or ١٢٨ bits, and using advanced mathematical calculations[١١],[١٢]. The efficacy of file encryption relies on the confidentiality of the key in use, as decryption is only possible along with the correct secret key [١٣]. Commonly utilized across diverse websites, block ciphers get the applications in data that transfer, store, anti-malware, and user privacy [١٤]. They encode data throughout transmission to prevent eavesdropping, safe and secure stored data on the devices, prevent the spread of malware and file encryption [١٥],[١٦], as well as safeguard confidential data like medical and fiscal documents, supporting the personal privacy of people and also institutions [١٧],[١٨]. Despite of the large number of different types of block ciphers, only some of them are known to the general public [١٩]. The most famous and in common use type of block cipher is the DES, ٣DES, and AES [٢٠],[٢١],[٢٢].

٢,١. The Triple Data Encryption Standard

٣DES was proposed as an enhancement to DES, providing a higher level of security [٢٣]. ٣DES features an increased key size and operates by applying the DES algorithm ٣ times to each data block. The key lengths for ٣DES are ١١٢ and ١٦٨ bits, with ٤٨ rounds, and it uses a ٦٤-bit block size [٢٤],[٢٥],[٢٦].This design offers heightened protection against cryptanalytic attacks, though the increased security comes at the cost of longer encryption time [٢٧],[٢٨].

٢,٢ Transposition Cipher

A transposition cipher is a method of cryptography where the sequence of characters in a message is rearranged without changing the characters, according to a designated system or key, disrupting the original character sequence to conceal the message's meaning [٢٩],[٣٠]. Transposition algorithms are primarily used for data encryption, and to guard sensitive information from unauthorized access [٣١]. While not typically used alone in modern cryptographic practices, transposition ciphers can form part of a larger, more complex encryption system [٣٢].

٣. Proposed System

This section presents an innovative encryption system that combines the traditional ٣DES algorithm and the transposition algorithm by adding a change in the key length in an intelligent manner to provide a robust and scalable security solution. The system aims to enhance data protection by leveraging the strengths of both algorithms, thereby increasing the complexity of the encryption process and improving the system's resistance to attacks.

٣,١ Propose algorithm

Here, we introduce and explain the main algorithms to ensure a focused approach toward achieving the desired goal.

Algorithm١ focuses on preparing and encrypting the file, including the necessary steps to handle file sizes, key generation, encryption methods, and data encapsulation. While **Algorithm٢** emphasizes the secure transmission of the encrypted data, including setting acknowledgment types, validating file status, and ensuring secure delivery to the destination.

Algorithm ١ : Encryption Process

Input: file (any file type and size), destination (user site)

Output: (cipher file, keys, block size)

١. Start

٢. Read the input file.

٣. Calculate the file size

٤. Select the block size based on the file size and cipher time that needed

- If file size < ١MB, block size = ٦٤.
- If file size < ١GB, block size = ١٢٨.
- If file size < ١TB, block size = ٢٥٦.

٥. Calculate the key length to improve security as:

- Pass one with specific key length
- pass two with another key length

٦. Apply encryption:

- Encrypt the data using the ٣DES algorithm with the key generated in Pass ١.
- Encrypt the data using a transposition algorithm with the key generated in Pass ٢.

٧. Create a table to record each user and their respective key variant values, based on file and user.

٨. Save data (block size and key lengths for pass ١ and pass ٢).

٩. Encapsulate Process:

Encapsulate_ data(cipher file, block size, key lengths for both passes and destination).

١٠. End

Algorithm ٢ : Sending Process

Input:

- encapsulated_data: The data structure resulting from the encryption process
- destination : The user's designated location
- file_status : Select either as a combination of sending and receiving status (including tracking information), or as a simple status indicating whether the file is 'crashed' or 'intact'."

Output:

- Acknowledgment_type

١. Start

٢. Rem" This step determines how the system confirms that the data has been successfully received. It may involve specifying different types of acknowledgments depending on the method of communication".

Set Acknowledgment Type(source, destination)

٣. Rem" This step prepares the data for transmission by ensuring that it is in the correct format and location for the transmission protocol"**.**

Insert Cipher in Section that designated for it

٤. Rem" This step prepares the data for transmission by ensuring that it is in the correct format and location for the transmission protocol".

Insert Data(block size, keys length pass ١ and pass ٢ ,destination)

٥. Rem" This step check File Status and Determine Acknowledgment type ":

a. If the file status is 'intact,' update the acknowledgment state to "Acknowledgment: Received."

b. Otherwise, update the acknowledgment type to compromised that's mean (take the necessary action).

٦. **Refresh Encapsulated Data with Acknowledgment type and send it Securely**

٧. End

٣,٢ implementation

In this section, a multilayer encryption system is utilized to improve file security by encrypting data in two consecutive passes using different algorithms and with variable key lengths. During the first phase, the ٣DES algorithm is applied using a key length that is determined by the system depending on the user. In the second phase, the transposition algorithm is implemented with a different key length that also depends on the user . This variation in algorithms and key lengths greatly enhances the complexity of the decryption process, making it harder for attackers to gain access to the data. In case of an attack, the key lengths are automatically modified to ensure ongoing protection without any intervention or awareness by

the system user. Table ١ shows the correlation between usernames and key lengths, while Table ٢ demonstrates the relationship between file size and block size.

User Name	Key 1 Length	Key 2 Length
1	6	4
2	3	9
3	7	8

Table 1

File Size	Block Size 1	Block Size 2
< 1M	64	64
< 1G	128	64
< 1T	256	128

Table 2

٤. Experimental Result

This section presents Figure ١.a, which represents the input to the ٣DES encryption algorithm, which is in the form of digital values and has a size of ١٢٨ bits (١٦x٨).

١	٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦
١٧															
٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧
١٨															
٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨
١٩															
٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩
٢٠															
٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠
٢١															
٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١
٢٢															
٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢
٢٣															
٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢	٢٣
٢٤															
٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢	٢٣	٢٤

Fig١.a. Input to the ٣DES Algorithm

And Figure ١.b illustrates the process of the transposition encryption for a block of size ١٢٨ x ١٢٨.

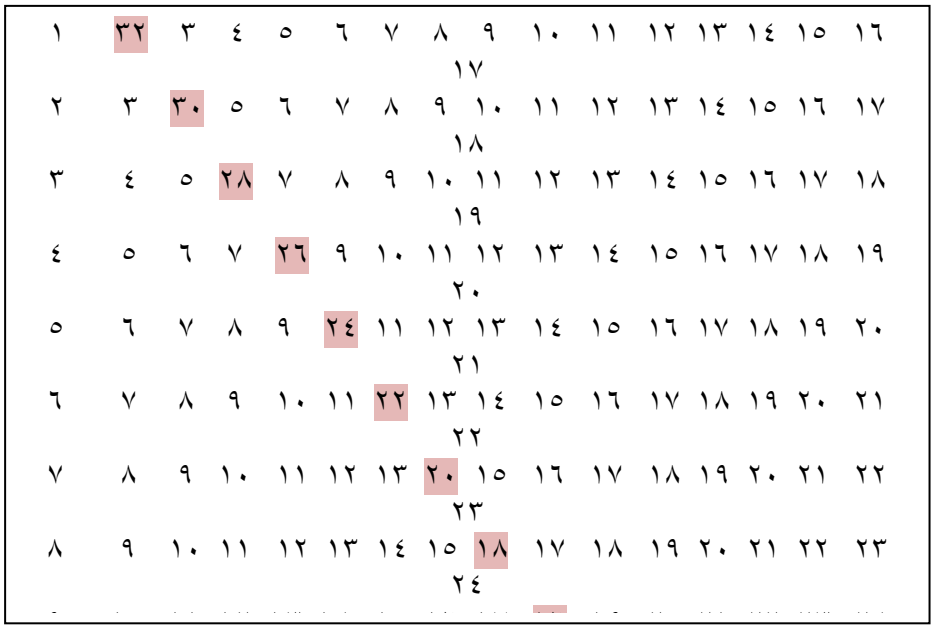

Fig ١.b. Process of Transposition Algorithm

Figure ٢.a represents the actual data after inserting a test file into the ٣DES encryption algorithm and taking a block segment of size ١٢٨ x ١٢٨. After that, the transposition algorithm is applied to the same encrypted segment, and the block segment is exposed in the format shown in Figure ٢.b.

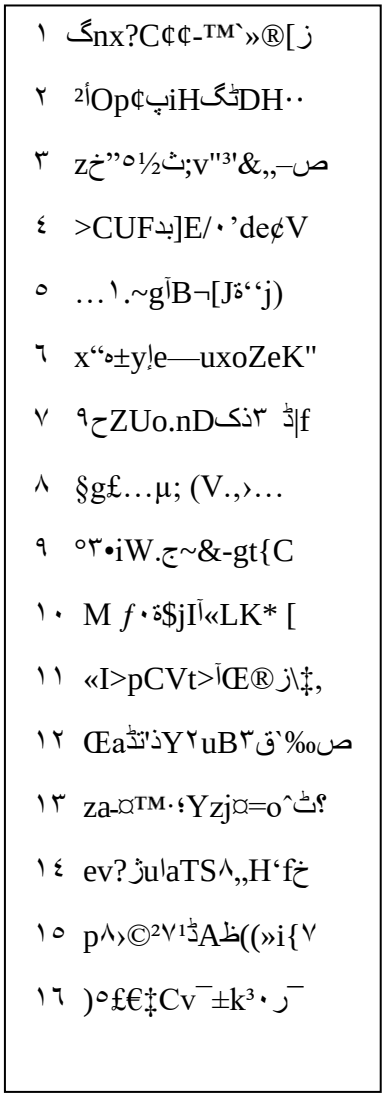

Figure ٢.a

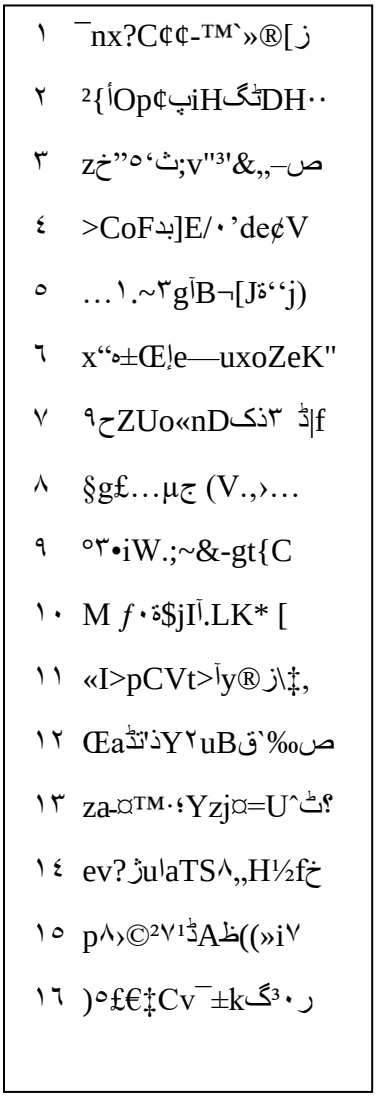

Figure ٢.b

Based on the data of Table ٣ in appendix , which represents the file size and the level of complexity based on the time required to decrypt it using simple decryption software approved by NIST cryptographic institutions, Figure ٣ illustrates the time required to decrypt a (١٢٨x١٢٨) block using the ٣DES algorithm.

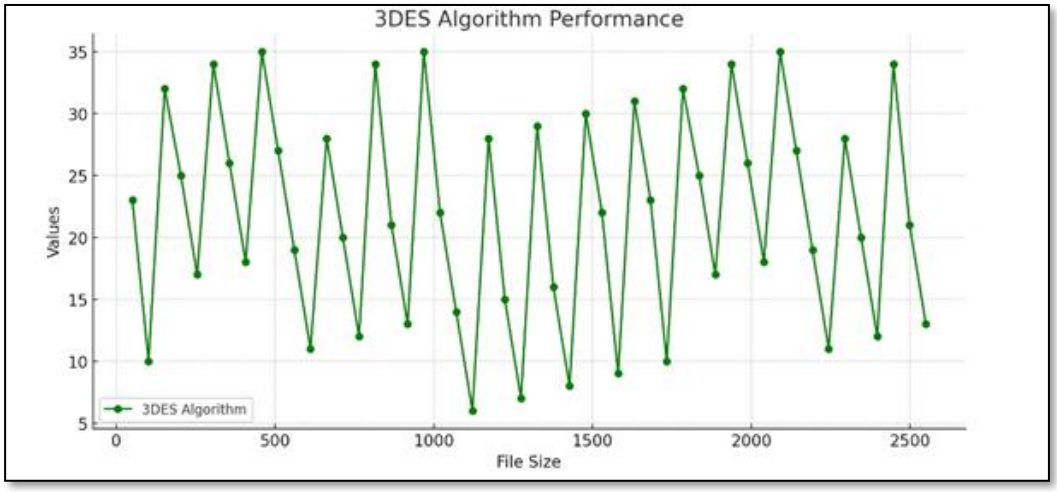

Figure ٣. Time Required to Decrypt by the ٣DES Algorithm

Figure ٤ illustrates the time required to decrypt a ١٢٨ x ١٢٨ block using the transposition algorithm.

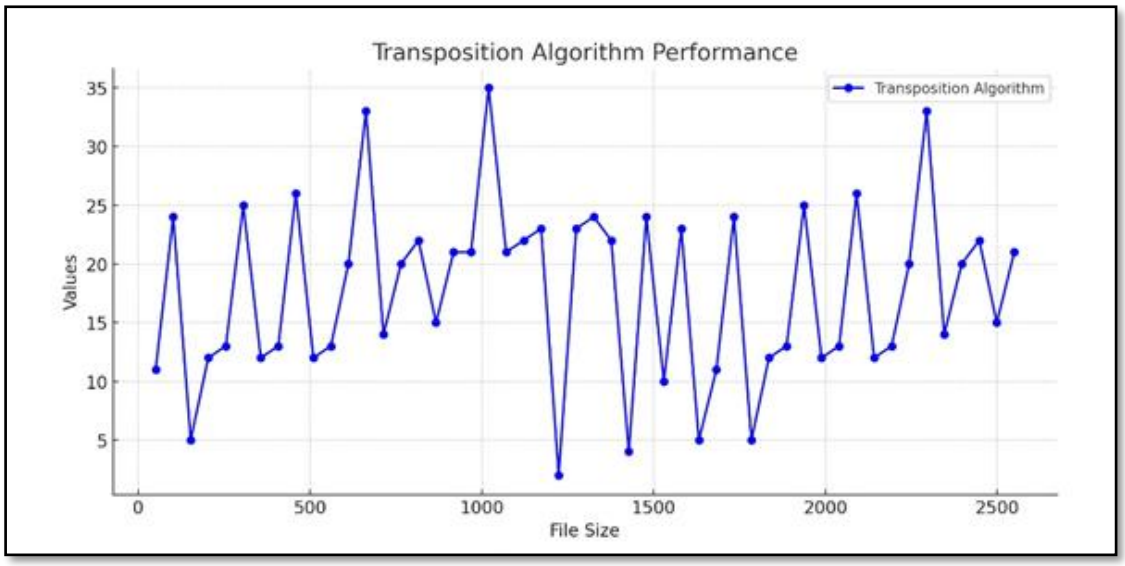

Figure ٤. Time Required to Decrypt by the transposition Algorithm

Figure ٥ illustrates the time required to decrypt a ١٢٨ x ١٢٨ block using the proposed algorithm.

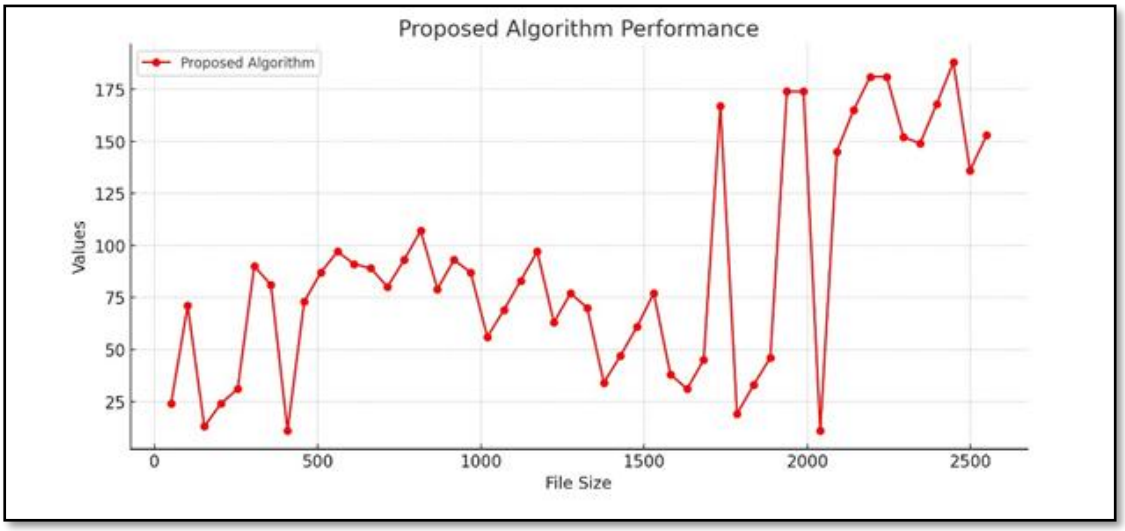

Figure ٥ Time Required to Decrypt by the Proposed Algorithm

Figure ٦ shows a comparison between three algorithms: ٣DES, the transposition algorithm, and the proposed algorithm, in terms of their complexity level based on decryption time. The comparison demonstrates that the proposed system performs better than the traditional ٣DES and transposition algorithms.

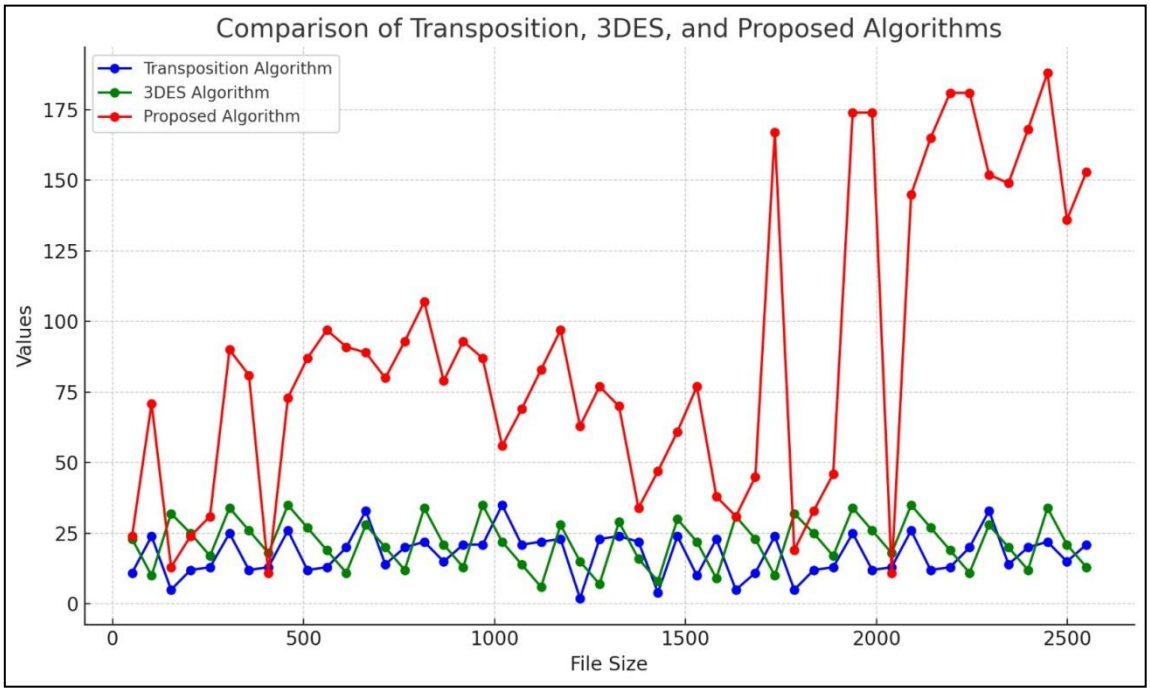

Figure ٦ Compare the Decoding time required by the Algorithms

٥.Conclusion

In this section, we will discuss the most prominent conclusions that were recorded through the application of the proposed system:

١. The proposed intelligent block cipher system demonstrated strong effectiveness in encryption by integrating ٣DES and transposition algorithms with key length change in an intelligent manner which effectively enhances data security.

٢. The proposed algorithm improved the efficiency and robustness of encryption and decryption operations, achieving up to ٩١٪ performance improvement in resistance to unauthorized access compared to traditional encryption methods.

٣. Data security complexity has increased, (making encryption harder to crack), due to a multi-stage encryption structure and dynamically changing key lengths.

References

[١] A. N. A. S. T. A. S. I. I. A. Bessarab, T. E. T. I. A. N. A. Hyrina, O. L. E. K. S. I. I. Sytnyk, N. A. T. A. L. I. A. Kodatska, O. L. H. A. Yatchuk, and L. I. U. D. M. Y. L. A. Ponomarenko, "The modern transformation of internet communications," J Theor Appl Inf Technol, vol. ١٠٠, no. ١٥, pp. ٤٧١٠–٤٧٢٢, ٢٠٢٢.

[٢] M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, and H. Al-Shahwani, "The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment," *Mesopotamian Journal of Cyber Security*, pp. ١–٦, Jan. ٢٠٢٣, doi: ١٠,٥٨٤٩٦/MJCS/٢٠٢٣/٠٠١.

[٣] P. Brauner *et al.*, "A Computer Science Perspective on Digital Transformation in Production," *ACM Transactions on Internet of Things*, vol. ٣, no. ٢, pp. ١–٣٢, May ٢٠٢٢, doi: ١٠,١١٤٥/٣٥٠٢٢٦٥.

[٤] T. Jordan, "The digital environment: How we live, learn, work, and play now. Boczkowski, Pablo J. and Mitchelstein, Eugenia. The <scp>MIT</scp> Press. ٢٠٢١. ٢٠٨ pp. $٢٤,٩٥ (hardcover). (<scp>ISBN</scp> : ٩٧٨٠٢٦٢٠٤٦١٩٠).," *J Assoc Inf Sci Technol*, vol. ٧٤, no. ٧, pp. ٨٧٩–٨٨١, Jul. ٢٠٢٣, doi: ١٠,١٠٠٢/asi.٢٤٧٥٢.

[٥] A. Nikiforova, "Data Security as a Top Priority in the Digital World: Preserve Data Value by Being Proactive and Thinking Security First," ٢٠٢٣, pp. ٣–١٥. doi: ١٠,١٠٠٧/٩٧٨-٣-٠٣١-١٩٥٦٠-٠_١.

[٦] F. Gandhi, D. Pansaniya, and S. Naik, "Ethical hacking: Types of hackers, cyber-attacks and security," *International Research Journal of Innovations in Engineering and Technology*, ٢٠٢٢.

[٧] S. A. Abead and N. H. M. Ali, "Lightweight Block and Stream Cipher Algorithm: A Review," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. ٥, no. ٢, pp. ٨٦٠–٨٧٤, Jun. ٢٠٢٤, doi: ١٠,٣٧٣٨٥/jaets.v٥i٢,٣٩٦٦.

[٨] W. Cai and H. Yao, "A Secure Transmission Method of Network Communication Data Based on Symmetric Key Encryption Algorithm," *Wirel Pers Commun*, vol. ١٢٧, no. ١, pp. ٣٤١–٣٥٢, Nov. ٢٠٢٢, doi: ١٠,١٠٠٧/s١١٢٧٧-٠٢١-٠٨٢٦٦-w.

[٩] A. A. Kuznetsov, O. V. Potii, N. A. Poluyanenko, Y. I. Gorbenko, and N. Kryvinska, *Stream Ciphers in Modern Real-time IT Systems*, vol. ٣٧٥. Cham: Springer International Publishing, ٢٠٢٢. doi: ١٠,١٠٠٧/٩٧٨-٣-٠٣٠-٧٩٧٧٠-٦.

[١٠] Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Generation Computer Systems*, vol. ١٥٧, pp. ٢٨٨–٣٠٢, Aug. ٢٠٢٤, doi: ١٠,١٠١٦/j.future.٢٠٢٤,٠٣,٠٥٤.

[١١] M. S. Naik, D. K. Sreekantha, and K. V. S. S. S. S. Sairam, "Comparative Study of Block Ciphers Implementation for Resource-Constrained Devices (Review)," *Radioelectronics and Communications Systems*, vol. ٦٦, no. ٣, pp. ١٢٣–١٣٧, Mar. ٢٠٢٣, doi: ١٠,٣١٠٣/S٠٧٣٥٢٧٢٧٢٣٠٥٠٠١١.

[١٢] amina Alregabo and Y. Hikmat Ismael, "BLOCK CIPHER PERFORMANCE AND RISK ANALYSIS," *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. ١٧, no. ١, pp. ٢٣–٣٣, Jun. ٢٠٢٣, doi: ١٠,٣٣٨٩٩/csmj.٢٠٢٣,١٧٩٤٦٣.

[١٣] A. K. K. Alregabo and Y. H. Ismail, "Proposed Method for Efficient Block Cipher Cryptography," *Eximia*, vol. ٩, pp. ١١–٢٤, Apr. ٢٠٢٣, doi: ١٠,٤٧٥٧٧/eximia.v٩i١,٢٤٥.

[١٤] R. Banoth and R. Regar, "Security Standards for Classical and Modern Cryptography," in *Classical and Modern Cryptography for Beginners*, Cham: Springer Nature Switzerland, ٢٠٢٣, pp. ٤٧–٨٣. doi: ١٠,١٠٠٧/٩٧٨-٣-٠٣١-٣٢٩٥٩-٣_٢.

[١٥] F. Varghese and P. Sasikala, "A Detailed Review Based on Secure Data Transmission Using Cryptography and Steganography," *Wirel Pers Commun*, vol. ١٢٩, no. ٤, pp. ٢٢٩١–٢٣١٨, Apr. ٢٠٢٣, doi: ١٠,١٠٠٧/s١١٢٧٧-٠٢٣-١٠١٨٣-z.

[١٦] Q. Wang *et al.*, "Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols," *Mathematical Biosciences and Engineering*, vol. ٢٠, no. ١١, pp. ١٩٩٨٣–٢٠٠٠١, ٢٠٢٣, doi: ١٠,٣٩٣٤/mbe.٢٠٢٣٨٨٥.

[١٧] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput Sci*, vol. ٣, no. ٢, p. ١٢٧, Mar. ٢٠٢٢, doi: ١٠,١٠٠٧/s٤٢٩٧٩-٠٢٢-٠١٠٢٠-٤.

[١٨] V. B. Komaragiri and A. Edward, "AI-Enhanced Information Security: Safeguarding Government and Healthcare PHI," *International Journal of Engineering and Computer Science*, vol. ١١, no. ٠٨, pp. ٢٥٦٠١–٢٥٦١٧, Aug. ٢٠٢٢, doi: ١٠,١٨٥٣٥/ijecs/v١١i٠٨,٤٦٩٧.

[١٩] M. A. Jimale *et al.*, "Authenticated Encryption Schemes: A Systematic Review," *IEEE Access*, vol. ١٠, pp. ١٤٧٣٩–١٤٧٦٦, ٢٠٢٢, doi: ١٠,١١٠٩/ACCESS.٢٠٢٢,٣١٤٧٢٠١.

[٢٠] R. Sood and H. Kaur, "A Literature Review on RSA, DES and AES Encryption Algorithms," in *Emerging Trends in Engineering and Management*, Soft Computing Research Society, ٢٠٢٣, pp. ٥٧–٦٣. doi: ١٠,٥٦١٥٥/٩٧٨-٨١-٩٥٥٠٢٠-٣-٥-٠٧.

[٢١] P. Parikh, N. Patel, D. Patel, P. Modi, and H. Kaur, "Ciphering the Modern World: A Comprehensive Analysis of DES, AES, RSA and DHKE," in *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, Feb. ٢٠٢٤, pp. ٨٣٨–٨٤٢. doi: ١٠,٢٣٩١٩/INDIACom٦١٢٩٥,٢٠٢٤,١٠٤٩٨٣٣٠.

[٢٢] C.-W. Cheng, M. H. Cantu, and S. Kumar, "Analyzing Computational Components of Standard Block Encryption Schemes," *Journal of Computer and Communications,* vol. ١٠, no. ٠٦, pp. ٨١–٨٩, ٢٠٢٢, doi: ١٠,٤٢٣٦/jcc.٢٠٢٢,١٠٦٠٠٧.

[٢٣] M. Jammula, "Comparative Study on DES and Triple DES Algorithms and Proposal of a New Algorithm Named Ternary DES for Digital Payments," *Asian Journal of Applied Science and Technology,* vol. ٠٦, no. ٠١, pp. ٨٩–٩٨, ٢٠٢٢, doi: ١٠,٣٨١٧٧/ajast.٢٠٢٢,٦١١١.

[٢٤] S. E. Anant and S. Varadarajan, "Information security with cryptography symmetric key encryption algorithms: a survey," *i-manager's Journal on Communication Engineering and Systems,* vol. ١١, no. ١, p. ١٩, ٢٠٢٢, doi: ١٠,٢٦٦٣٤/jcs.١١,١,١٨٩١٣.

[٢٥] S. M. Radhi and R. Ogla, "In-Depth Assessment of Cryptographic Algorithms Namely DES, ٣DES, AES, RSA, and Blowfish," *Iraqi Journal of Computer, Communication, Control and System Engineering,* pp. ١٢٥–١٣٨, Sep. ٢٠٢٣, doi: ١٠,٣٣١٠٣/uot.ijccce.٢٣,٣,١١.

[٢٦] S. M. MOHD *et al.*, "THE PERFORMANCE OF THE ٣DES AND FERNET ENCRYPTION IN SECURING DATA FILES," *J Theor Appl Inf Technol,* vol. ١٠٢, no. ٣, ٢٠٢٤.

[٢٧] C. Tezcan, "Key lengths revisited: GPU-based brute force cryptanalysis of DES, ٣DES, and PRESENT," *Journal of Systems Architecture,* vol. ١٢٤, p. ١٠٢٤٠٢, Mar. ٢٠٢٢, doi: ١٠,١٠١٦/j.sysarc.٢٠٢٢,١٠٢٤٠٢.

[٢٨] B. Sarkar, A. Saha, D. Dutta, G. De Sarkar, and K. Karmakar, "A Survey on the Advanced Encryption Standard (AES): A Pillar of Modern Cryptography," *International Journal of Computer Science and Mobile Computing,* vol. ١٣, no. ٤, pp. ٦٨–٨٧, Apr. ٢٠٢٤, doi: ١٠,٤٧٧٦٠/ijcsmc.٢٠٢٤.v١٣i٠٤,٠٠٨.

[٢٩] B. Al-Kasasbeh, "A Novel Secure Transposition Cipher Technique using Arbitrary Zigzag Patterns," *International Journal of Advanced Computer Science and Applications,* vol. ١٣, no. ١, ٢٠٢٢, doi: ١٠,١٤٥٦٩/IJACSA.٢٠٢٢,٠١٣٠١٣٣.

[٣٠] A. Armah, S. Asare, and E. Abrefah-Mensah, "Enhancing Security in Modern Transposition Ciphers Through Algorithmic Innovations and Advanced Cryptanalysis," *Indonesian Journal of Computer Science,* vol. ١٣, no. ٣, Jul. ٢٠٢٤, doi: ١٠,٣٣٠٢٢/ijcs.v١٣i٣,٤٠٩٥.

[٣١] William Easttom, *Modern cryptography: applied mathematics for encryption and information security,* Second. ٢٠٢٢.

[٣٢] R. Banoth and R. Regar, *An Introduction to Classical and Modern Cryptography*. Springer Nature Switzerland., ٢٠٢٣.

Appendix

Table ٣ represents the file size and complexity rate based on the time required to decrypt it using simple decryption software approved by NIST cryptographic institutions.

File Size	Transposition alg.	٣DES alg.	Proposed alg.
٥١	١١	٢٣	٢٤
١٠٢	٢٤	١٠	٧١
١٥٣	٥	٣٢	١٣
٢٠٤	١٢	٢٥	٢٤
٢٥٥	١٣	١٧	٣١
٣٠٦	٢٥	٣٤	٩٠
٣٥٧	١٢	٢٦	٨١
٤٠٨	١٣	١٨	١١
٤٥٩	٢٦	٣٥	٧٣
٥١٠	١٢	٢٧	٨٧
٥٦١	١٣	١٩	٩٧
٦١٢	٢٠	١١	٩١
٦٦٣	٣٣	٢٨	٨٩
٧١٤	١٤	٢٠	٨٠
٧٦٥	٢٠	١٢	٩٣
٨١٦	٢٢	٣٤	١٠٧
٨٦٧	١٥	٢١	٧٩
٩١٨	٢١	١٣	٩٣
٩٦٩	٢١	٣٥	٨٧
١٠٢٠	٣٥	٢٢	٥٦
١٠٧١	٢١	١٤	٦٩
١١٢٢	٢٢	٦	٨٣
١١٧٣	٢٣	٢٨	٩٧
١٢٢٤	٢	١٥	٦٣
١٢٧٥	٢٣	٧	٧٧
١٣٢٦	٢٤	٢٩	٧٠
١٣٧٧	٢٢	١٦	٣٤
١٤٢٨	٤	٨	٤٧
١٤٧٩	٢٤	٣٠	٦١
١٥٣٠	١٠	٢٢	٧٧
١٥٨١	٢٣	٩	٣٨
١٦٣٢	٥	٣١	٣١
١٦٨٣	١١	٢٣	٤٥
١٧٣٤	٢٤	١٠	١٦٧
١٧٨٥	٥	٣٢	١٩
١٨٣٦	١٢	٢٥	٣٣
١٨٨٧	١٣	١٧	٤٦
١٩٣٨	٢٥	٣٤	١٧٤
١٩٨٩	١٢	٢٦	١٧٤
٢٠٤٠	١٣	١٨	١١
٢٠٩١	٢٦	٣٥	١٤٥

١٦٥	٢٧	١٢	٢١٤٢
١٨١	١٩	١٣	٢١٩٣
١٨١	١١	٢٠	٢٢٤٤
١٥٢	٢٨	٣٣	٢٢٩٥
١٤٩	٢٠	١٤	٢٣٤٦
١٦٨	١٢	٢٠	٢٣٩٧
١٨٨	٣٤	٢٢	٢٤٤٨
١٣٦	٢١	١٥	٢٤٩٩
١٥٣	١٣	٢١	٢٥٥٠

Table ٣