Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (**PRINT**); 2705-3121 (**ONLINE**) **Research Article**

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index

DOI: https://dx.doi.org/10.4314/cajost.v6i1.14

Article Info

Received: 16th October 2023

Revised: 29th March 2024

Accepted: 30th March 2024

Comparative Analysis of Encryption Algorithms Using Simulation Technique

Aminu S. Yabo[1*], Mansur Aliyu[2], Salihu G. Auyo[3], Amiru Ali[4], Abdullahi M. Haruna[5], and Bashar F. Rugga[6]

[1]Department of Computer, Umaru Ali Shinkafi Polytechnic, Sokoto Nigeria.

[2]Department of Computer, Sokoto State University, Sokoto Nigeria.

[3,4,5]Department of Computer, Jigawa State Polytechnic, Duste Nigeria.

[6]CIT Unit, Kebbi State Polytechnic, Dakin-Gari, Kebbi Nigeria.

***Corresponding author's email:**

aminuyabo@gmail.com

Cite this: *CaJoST,* 2024, 1, 109-112

The unprotected electronic document may be subjected to a data breach in which private or sensitive information is stolen, taken, altered, copied, communicated, viewed, or used without authorization. This study evaluates the four most common encryption algorithms like Data Encryption Standard (DES) Algorithms, Rivest Cipher2 Algorithm (RC2), Triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). This aims to compare four (4) encryption algorithms using simulation in VB.NET programming approach that uses time and data size parameters to encrypt and decrypt data with greater efficiency. The simulation comparison technique using the VB.Net programming was adopted as the method for the study. A graphical user interface (GUI) was developed, and four algorithms were programmed to evaluate their performance based time and data size. As a result, the four Encryption Algorithms were evaluated and found that the Advanced Encryption Standard algorithm (AES) performs much faster in VB.Net.

Keywords: Electronic Code Book, Simulation Comparison Technique, Graphical user Interface.

1. Introduction

Taha et al. (2019), the science or study of methods for secret writing and concealing communications in any medium is known as cryptography. Encryption converts a plaintext or piece of data into a ciphertext, which prevents nefarious outsiders from deciphering the content. Qui et al. (2019), the importance of knowledge and, more recently, data has increased, accelerating the development of cryptography. The requirement for secret military communication then impacted the first known encryption, which had been used to safeguard religious or commercial information. The need for safe business and private communication brought about the following significant modifications. Computers and the internet have progressively taken over our life since the 1980s. Therefore, communication between people, machines, or people and machines is best encrypted in the Information Age.

According to Li et al., advances in information technology bring us ease and efficiency and new information security issues (2019). More people can only access information services with secure data transfer. Chandramouli & Pinhas (2020) argue that data encryption is a fundamental security method used to protect computer data stored outside of system memory to stop data theft and other malicious activities. Encrypted data makes essential documents much more secure as it makes them difficult to decrypt, even if lost or leaked. Hafen et al. (2019), the history of simulation can be written from a variety of angles, including the uses of simulation (analysis, training, and research), types of simulation models (discrete-event, continuous, combined discrete-continuous), simulation programming languages or environments (GPSS, SIMSCRIPT, SIMULA, SLAM, Arena, Auto Mod, Simio), and application domains or communities of interest (communications, manufacturing, military, transportation). Examples of the many viewpoints and combinations are easily accessible in the histories that have been published; Nance (1996), Sergent et al. (2002), and Hollocks (2006).

The development of computer simulation began during World War II when mathematicians Jon Von Neumann and Stanislaw Ulam had to solve the perplexing issue of neutron behavior. Hit-and-miss experiments were too expensive, and the problem must be analyzed appropriately. So, the mathematicians proposed the Roulette wheel method. The probabilities of distinct occurrences were combined into the fundamental information about the likelihood of their occurrence in a step-by-step analysis to forecast the result of the entire series of events. Due to the exceptional performance of the neutron problem approaches, they quickly gained popularity and were used extensively in business and industry.

2. Methodology

In respect of the study conducted based on comparative methodologies for encryption algorithms, the researcher adopts the “Simulation Comparison Technique” to compare four encryption algorithms.

2.1 Rationale Behind the Selection of Simulation Comparison Technique

Vazan (2021), in his research to compare the speed of cryptography algorithms, expressed that using VB.Net simulation assists the researchers in locating obstructions in the flow of data, information, and other files easily. The simulation also enables an understanding more crucial factors, notably algorithm performance evaluation. Moreover, his research expressed that the simulation method of comparison aids his study in which he compares various solutions and designs using simulation by evaluating the performance of existing algorithms and forecasting the performance and concludes that simulation has the following benefit to adopting over the rest of the comparing methods: Speed, Easy to use and Accuracy.

2.2 How SCT is Implemented in this Study

i. In SCT GUI, a 64-bit plaintext block was used in the first transform operation at the operation's starting point.

ii. Plain text will then be subject to the first permutation (IP).

iii. The initial permutation (IP) was used to separate the accepted block into the correct plaintext (RPT) and left plaintext (LPT). Each LPT will go through the alteration procedure 16 times.

iv. The simulation procedure was then repeated 16 times for the LPT and RPT.

v. Finally, the newly combined block passed through Final Permutation once the LPT and RPT re-join (FP).

vi. The simulation process resulted in the creation of the necessary 64-bit cipher text.

2.3 How Vb.Net is Used in this Research

i. Using the VB.Net programming environment, a GUI or simulation system was developed.

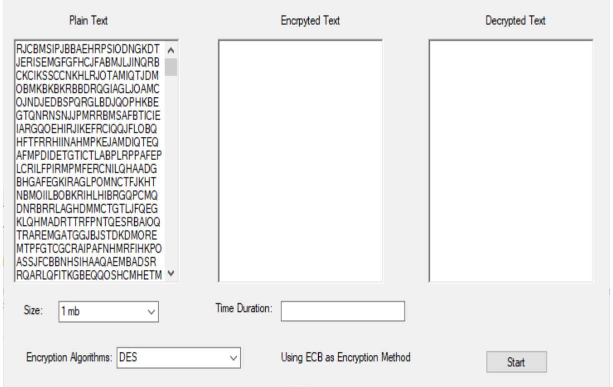
ii. The four encryption algorithms (DES, RC II, 3DES and AES) were programmed within the GUI for comparison.

iii. The simulation interface has a robust feature for real-world simulation

iv. The GUI was split into three sections: plaintext, encryption mode, decrypted text

2.4 Source of Data

Using SCT, the simulation system (GUI) was developed to compare four encryption algorithms: DES, RC II, 3DES and AES. The system generates plain text and allows the researcher to select an algorithm to determine its performance using time and data size (speed) during the simulation process. The system provides results based on time spent by a particular algorithm. Hence the researcher determines the faster algorithm.



```
RJCBMSIPJBBAEHRPSIODNGKDT
JERISEMGFGFHCJFABMJLJINQRB
CKCIKSSCCNKHLRJOTAMIQTJDM
OBMKBKBKRBBDRQGIAGLJOAMC
OJNDJEDBSPQRGLBDJQOPHKBE
GTQNRNSNJJPMRRBMSAFBTICIE
IARGQOEHIRJIKEFRCIQQJFLOBQ
HFTFRRHIINAHMPKEJAMDIQTEQ
AFMPDIDETGTICTLABPLRPPAFEP
LCRILFPIRMPMFERCNILQHAADG
BHGAFEGKIRAGLPOMNCTFJKHT
NBMOIILBOBKRIHLHIBRGQPCMQ
DNRBRRLAGHDMMCTGTLJFQEG
KLQHMADRTTRFPNTQESRBAIOQ
TRAREMGATGGJBJSTDKDMORE
MTPFGTCGCRAIPAFNHMRFIHKPO
ASSJFCBBNHSIHAAQAEMBADSR
RQARLQFITKGBEQQOSHCMHETM
```

Size: 1 mb

Encryption Algorithms: DES

Using ECB as Encryption Method

Figure 2.1 SCT G.U.I

3. Results and Discussion

3.1 Results

The outcomes of using various data loads to run the simulation program are displayed in this section. The effects of changing the data size on each approach for each investigated algorithm (DES, 3DES, AES, and RC2) are displayed in the figure below.

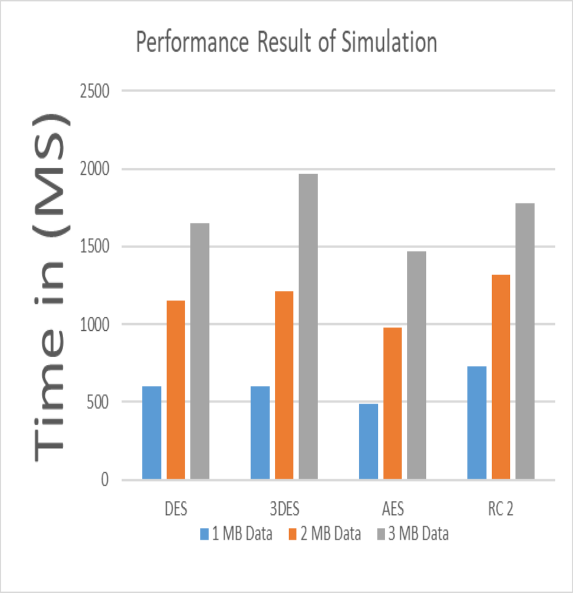


Figure 3.1 Result

3.2 Discussion

The study compares four encryption algorithms using a simulation comparison method to determine which algorithm encrypts and decrypts data in VB.Net more quickly at various data sizes. Based on the fastest algorithm after comparison, the study recommends the best algorithm to guarantee the security and integrity of data in real-time. Using a simulation comparison method with VB.NET, the four most widely used encryption algorithms, Advanced Encryption Standard (AES), Rivest Cipher2 Algorithm (RC2), Data Encryption Standard (DES), and Triple Data Encryption Standard (3DES), have been assessed. AES is the fastest encryption/decryption algorithm in VB.NET programming. Based on the comparison, AES was the fastest encryption/decryption algorithm in VB.NET programming. By storing a document in an encrypted format that can only be retrieved by providing the right password supplied while cryptography, the AES algorithm supports all new encryption/decryption software functions, making it the best algorithm in terms of performance. Additionally, AES's performance (speed) improves as the Data Size increases, which cuts down on processing time.

3.3 Recommendation

The Advanced encryption standard (AES) algorithm is recommended for secured transmission of data over internet and other modes of data communication due it quicker encryption and decryption. This back Agbelusi and Matthew (2023) in their study comparative analysis of Encryption algorithms using Java programming.

4. Conclusion

This study has demonstrated the effectiveness of the VB.Net simulation comparison technique. This study's VB.Net simulation approach produces the fastest algorithm in terms of data security. Advanced Encryption Standard (AES) was contrasted with DES, 3DES, and RC2 to select the quickest algorithm. To assess performance: time and data size parameters in milliseconds in various data size (MB), the simulation was run in Electronic Code Book Mode (ECB), which uses the AES symmetric technique (key to key cryptography). It's pertinent to note that, due to its three-phase encryption operation, 3DES often requires more time than RC2. AES works better than DES and other encryption techniques despite having a lengthy key (256 bits). The results had little to do with other loads operating on the computer because each experiment was carried out several times and produced almost similar results to what was anticipated.

Conflict of interest

The authors declare no conflict of interest.

Authors' Contributions

AS Yabo conceived the overall development of the SCT Graphical user interface, integration of the algorithms in G.U.I and also prepared the manuscript. Mansur Aliyu assisted and supervised the study while Salihu Garba Auyo handled Analysis using data analysis tool. Also Amiru Ali and Abdullahi M. Haruna contributed in implementation of SCT with VB.Net Programming. Finally, B.F. Rugga studied various simulation method and recommended the SCT method.

Acknowledgements

All thanks and praises be Almighty God, the creator of the heavens and the earth, I thank him for preserving my life and giving me good health, wisdom and strength to conduct this research. I sincerely acknowledge with gratitude the important contributions of my supervisor Prof Mansur Aliyu to whom I am indebted, for his understanding, patience, recommendations, corrections and encouragement, which brought out the best in me; I am grateful, sir. I want to acknowledge and appreciate the efforts of co-researchers for their inputs. Finally, my indebtedness goes Caliphate Journal of Science and Technology (CaJoST) for considering my research worthy of publication.

References

[1] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of Steganography and Cryptography: A Short Survey. *In IOP Conference Series: Materials Science And Engineering* (Vol. 518, No. 5, p. 052003). IOP Publishing. **DOI 10.1088/1757-899X/518/5/052003**

[2] Qui, H., Kapusta, K., Lu, Z., Qiu, M., & Memmi, G. (2019). All-or-nothing data protection for ubiquitous communication*: Challenges and perspectives. Information Sciences*, 502, 434-445. **DOI: https://doi.org/10.1016/j.ins.2019.06.031**

[3] Li, D., Deng, L., Lee, M., & Wang, H. (2019). IoT Data Feature Extraction And Intrusion Detection System For Smart Cities Based on Deep Migration Learning. *International Journal of Information Management*, 49, 533-545. **DOI: https://doi.org/10.1016/j.ijinfomgt.2019.04.006**

[4] Chandramouli, R., & Pinhas, D. (2020). Security Guidelines for Storage Infrastructure. *NIST Special Publication*, 800, 209. **DOI: https://doi.org/10.6028/NIST.SP.800-209**

[5] Hafen, Z., Faucher-Giguere, C. A., Anglés-Alcázar, D., Stern, J., Kereš, D., Hummels, C., & Murray, N. (2019). The origins of the circumgalactic medium in the FIRE simulations. *Monthly Notices of the Royal Astronomical Society*, 488(1), 1248-1272. **DOI: https://doi.org/10.1093/mnras/stz1773**

[6] Nance, R. E. (1996). A history of discrete event simulation programming languages. *In History of Programming Languages II* (pp. 369-427). **DOI: https://doi.org/10.1145/234286.1057822**

[7] Sergent, F., Paiella, R., Martini, R., Colombelli, R., Gmachl, C., Myers, T. L., ... & Whittaker, E. A. (2002). Quantum cascade lasers: ultrahigh-speed operation, optical wireless communication, narrow linewidth, and far-infrared emission. *IEEE Journal of quantum electronics*, 38(6), 511-532.

[8] Hollocks, B. W. (2006). Forty years of discrete-event simulation. *A personal reflection. Journal of the Operational Research Society*, 57, 1383-1399. **DOI: https://doi.org/10.1057/palgrave.jors.2602128**

[9] Vazan, K. M. (2021). Comparative analysis on the speed of Algorithms. *International journal of computer and mathematical theory*, 135, 12845.

[10] Agbelusi, O., & Matthew, O. (2023). Comparative analysis of Encryption Algorithms. *European Jounal of Technology*, Vol.7 issue 1, pp 1 – 9. **DOI: https://doi.org/10.47672/ejt.1312**