University of Ibadan
Journal of Science and Logics in ICT Research

Enhancing Data Security: Implementing a Step-Count Method for Confidential Communications during Practical Transmission

Adeyemi I. O.[1], Akinola S. O.[2], Olagunju S. K.[3] and Omotosho F. S.[4]
[1]*isreal.adeyemi@koladaisiuniversity.edu.ng*, [2]solom202@yahoo.co.uk,
[3]olagunjukoredesolomon@gmail.com, [4]funshosegun10@gmail.com
[1,3,4]*Department of Computer Science, Koladaisi University, Ibadan, Nigeria*
[2]*Department of Computer Science, University of Ibadan, Nigeria*

Abstract
Overall, the improved structure of the data encryption standard algorithm delivers a state-of-the-art solution for protecting confidential data backed by unrivaled expertise and meticulous design. It is an essential tool in today's digital landscape, where cybersecurity threats are ever-evolving. Encryption is the encoding of a statement that only trusted parties can read. Only the authorized recipient understands the encoded message. The research aims to develop a step-count data encryption model for minimizing information breaches in transmission. In this research, the "key" length is the same as the original dataset, the cipher length is equal to the original message, and it has a reduction in encrypting and decrypting times compared to the RSA algorithm.

Keywords: Encryption key, Encryption, Cipher text, Block cipher, Decryption

1. Introduction

Transmitting to each other has been human essence since it was here on earth. Human transmission serves as a means to comprehend one another. The evolution of technology and media to disseminate from ancient times until now continues to experience growth before the devices to report information, transmitting information from one location to another. The history of encryption emanated about 600 BC when the ancient Spartans used a scytale appliance to transmit secret notices during battle. Encryption is the process of modifying the actual data into secret data. Decryption is the act of changing confidential data into authentic data. Zahraa *et al.* [1] wrote that data protection is a complex problem affecting areas of communication. They compared symmetric and asymmetric encryption methods.

Encryption is an intricate mathematical mechanism predominantly used for cloaking data and transmissions to guarantee that they are not accessed or meddled with by unauthorized persons. A simplified description is that encryption and decryption data require keys to lock and unlock the data. When attackers try to get this data in encrypted form without the key, it is ungrammatical and useless to them. Encryption is not as effortless as it sounds, and its general use has a "key" problem with basic usability.

The research requires the implementation of changes in "key" attributes of the improved structure of the algorithm. These include an increased key size and more complex permutation functions, making it harder for unauthorized individuals or systems to decipher encrypted data. Overall, the improved structure of the Data Encryption Standard algorithm provides a higher level of security for sensitive data, allowing organizations to safeguard their valuable information from malicious threats.

1.1 RSA Encryption Method

It is consistently necessary to provide suitable security assistance to any communication. The creation of the RSA technique brings momentous progress in cryptography. Until then, the accomplishment was only symmetric key cryptography, which employed only a key for encrypting and decrypting. Hence, the researchers have shown interest in devising similar algorithms that achieve some

Adeyemi I. O., Akinola S. O., Olagunju S. K. and Omotosho F. S. (2024). Enhancing Data Security: Implementing a Step-Count Method for Confidential Communications during Practical Transmission, *University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR)*, Vol. 12 No. 2, pp. 12 - 17

momentum over some time. RSA technique has a problem of computation. Santos and Junior [2] improved the Caesar method by demonstrating the possibility of modifying the method according to the security needs of the data in question. However, they noted the limitation of the technique in the face of brute force attacks. Nurcahya and Nazelliana [3] studied Vigenere Cipher, a prominent polyalphabetic substitution strategy to secure alphabetic text. They pointed out that it can only encrypt alphabetic letters and does not discriminate between upper and lower case. If the key length is shorter than the plaintext, it repeats the key, which can introduce patterns detectable by cryptanalysts**.**

2. Related Works

The data encryption standard algorithm has undergone enhancements in its structure, resulting in improved security and efficiency. These updates have been carefully considered and implemented by expert professionals to ensure the highest level of protection for sensitive data. Nevertheless, data breaches occur through exposure to sensitive information. Some idle individuals search for information to gossip about, disseminate unlawfully, or impersonate someone. They spy through the window, walk around without a basis in reason, or enter offices unnecessarily to get information. In the academic setting and a relationship, information needs restriction to specific individuals. Alteration in data results in a loss of trust, and it may lower confidence in systems.

Researchers used techniques like data encryption standard, advanced encryption standard algorithm, and Rivest Shamir algorithm (RSA) for encrypting and decrypting. RSA is not ideal for chatting. It takes time to decrypt the cipher text. Once the intruder gets the key, they can decrypt the cipher text. There is a need to develop a step-count approach that improves data encryption standards. The study concentrated on four concepts:

- The key,
- Encryption time,
- The ciphertext block,
- Decryption time.

Mays [4] enhanced the structure of the Data Encryption Standard using the classic Data Encryption Standard with a new form of two-key creation. It means that the "key" generation technique yields two keys: one is easy, and the other is encrypted using a sweetened Caesar method. The encryption technique in the first eight rounds employs an easy key one, and from round nine to round sixteen, the approach utilizes encrypted "key" two. Using the enhanced design of the Data Encryption Standard algorithm, the outcomes of this paper advance Data Encryption Standard encryption guard, rendition, and elaborateness of inquiry likened with classic Data Encryption Standard.

Khairul and Jefril [5] wrote that encryption is changing original data into secret data that is hard to read. They created a file system for encryption and decryption. Meanwhile, the decryption transforms personal data back into the original data. In this case, the Advanced Encryption Standard (AES) algorithm is the latest cryptographic technique standard. The previous algorithm could not cater to the developmental question of communication technology. AES is a cryptographic method using the Rijndael approach that can encrypt and decrypt data chunks over 128 bits with a "key" size of 128 bits.

Pronika [6] wrote that there are billions of internet users globally. They disseminate their details over the same because people consciously attempt to steal personal data. It is consistently advisable to transfer and keep data in encrypted format. They examined diverse encryption and decryption approaches and compared them concerning the time taken for encrypting and decrypting various proportions of files.

3. Methodology

Figure 1 describes the sender sending messages to a person without interruption. It allows the user to use a set of character, generate a key, and apply a step-count approach to generate a ciphertext for the receiver.

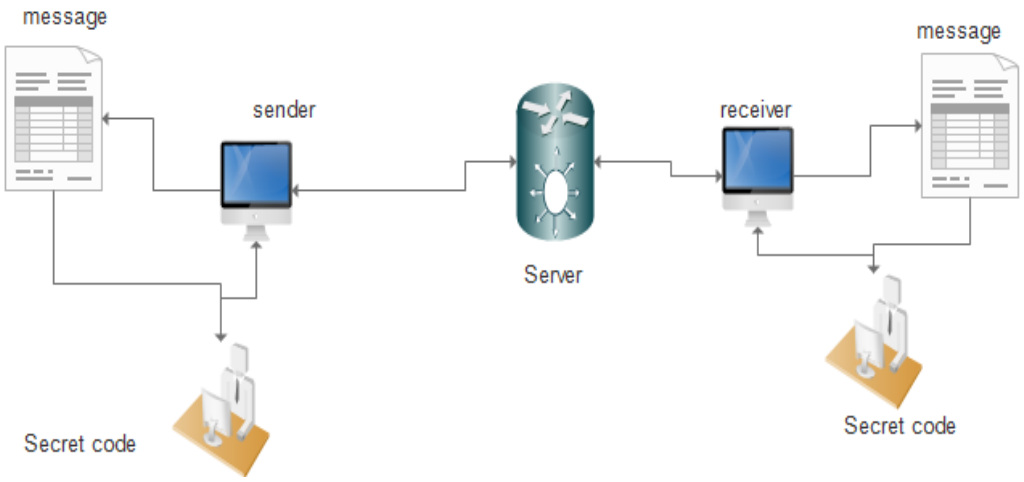

Figure 1: Model Architecture

There is a need to improve the data encryption standard (DES) algorithm to enhance its structural integrity and security. This updated version incorporates robust mechanisms to protect against unauthorized access and maintain the confidentiality of sensitive information. The work will improve the DES algorithm through thorough analysis and rigorous testing to provide enhanced protection for data at rest and in transit. By implementing these, there will be data protection from potential threats and breaches. With this improved structure, the DES algorithm remains a trusted method for secure data encryption in professional settings. Assume y is a set of alphabet, s is the step, k is the key, x is the set of inputs then:

$$A = y(x) \quad (1)$$

Equation 1 takes a set of strings relative to a set of inputs.

.

$$c = (p + s) \bmod y \quad (2)$$

Equation 2 computes the steps of Equation 1.

$$c = c + y(c) \quad (3)$$

Equation 3 keeps appending the ciphertext until there is no more character.

Figure 2 describes the implementation of the Figure 1. It shows the application of a step-count method to data before transmitting to the receiver.

3.1 Data source

The data is the alphabet, numbers, spaces, and special characters. The model takes a counter and relates it with the input characters. The step has a trace-back bit. It relates the key to the characters to generate cipher text.

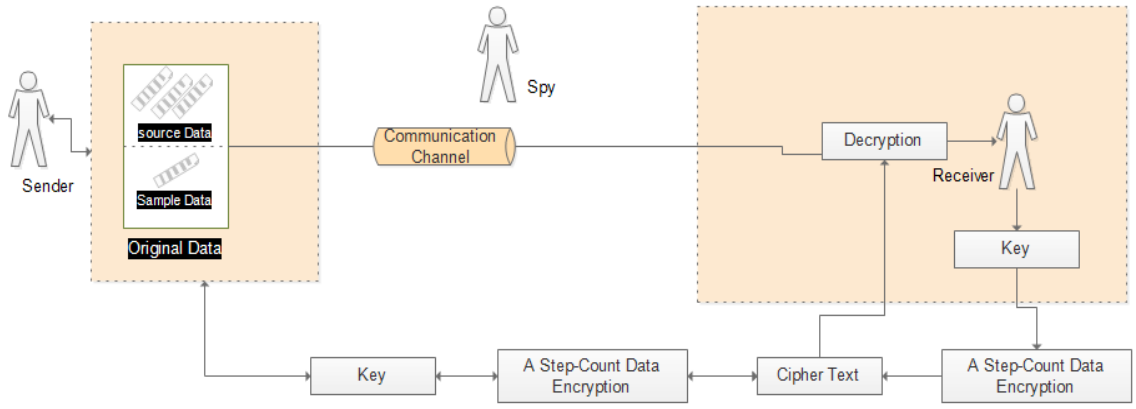

Figure 2: A Step-Count Data Encryption/Decryption Model

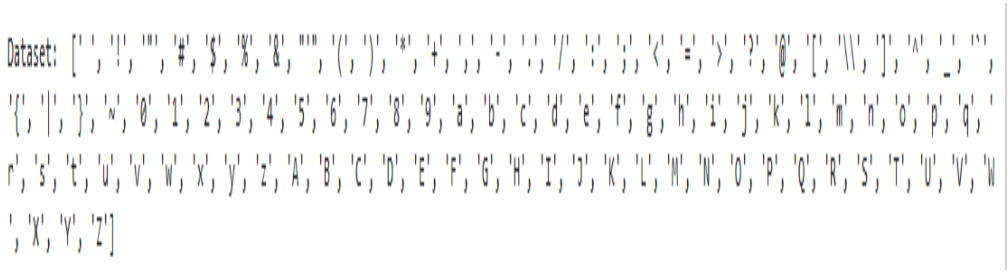

Figure 3: Dataset

Discovering publicly known data of encrypted messages with their related plaintexts can be demanding due to security and privacy concerns. However, the research utilizes the original dataset.

3.2 Analytical Process

There are considerable encryption methods, each of which varies by application and protection index. In this work, the dataset corresponds to some encryption algorithms, which require mathematical calculations as stated in equation 1 to equation 3. The algorithm takes each character of the word and counts the considerable steps in the key. The character of the key replaces the plaintext. In decrypting, the algorithm reverses the key and traces the plaintext to get the exact message. It follows a symmetric encryption standard.

3.3 Research Algorithm

Data: xi
Result: C(x)
Result: D(x)
Begin
 /* Define all strings */
 Set strings of data to integers

 /* Feature Mapping*/
 Define a key relative to the strings

 /* Define a loop for encrypting*/
 for string in input
 Find the string index
 Count step relative to the key
 Return cipher Text

 /* Define a loop for decrypting*/
 for cipher in input
 Find the cipher index
 Count step inverse relative to the key
 return message
End

3.4 Feature Extraction

Encryption feature extraction involves recognizing and investigating specific attributes of encrypted data to gain insights without decrypting the data. This process is functional in cryptography, cybersecurity, and data investigation. Here are some key ideas and techniques involved in encryption feature extraction:

Key-Length Estimation: Assess the scope of the encryption key based on the size of the ciphertext and other available parameters.

Algorithm Identification: Use known features of encryption algorithms to determine the algorithm used.

Timing Analysis: Calculate the time taken for encryption procedures to deduce details about the encryption process.

4 Results and Discussion

The latest data encryption standard algorithm boasts a more robust architecture, incorporating advanced encryption techniques such as "key" scheduling, permutation, substitution, and feedback mechanisms. This refined structure allows for cryptographic strength and resilience against potential attacks. Additionally, the updated algorithm features greater flexibility in terms of key length and block size options, allowing for customizable levels of security depending on specific needs and requirements.

Figure 4 is the interface for encrypting messages. The user supplies the strings of characters, and the system turns them into unreadable text.

Figure 5 is the interface for decrypting messages. The user pastes the cipher text, and the system turns it into a readable message.

4.1 Performance Evaluation

Table 1 shows that the step-count model performs better than RSA. The RSA approach has a higher execution time compared to the step-count model.

4.2 Discussion

The study shows that the core of the model counts on the 'key' association, numeral of keys, and digit of details used in a key. All the keys count upon the mathematical effects. The RSA approach requires more computation time, which indicates that the design positions more work to shuffle the data. A step-count data encryption method is an even better mathematically strong formation. The research compares the step-count algorithm with RSA, relating the time taken for encrypting and decrypting various sizes of messages.

5 Conclusion

The research provides security because it is difficult for spies to know the steps to generate the cipher text. Encryption methods take a significant time and storage, but the step-count data standard encryption minimizes these limitations. The results reveal a reduction in computation time and cipher text.

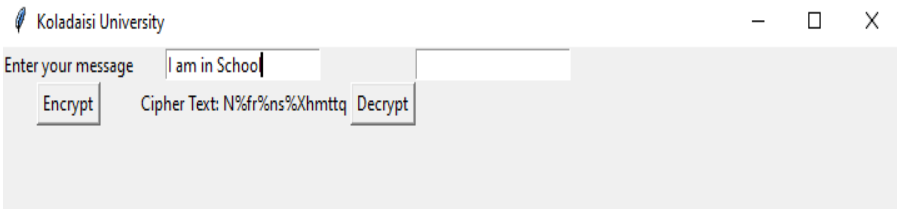

Figure 4: A Step-count Data Standard Encryption

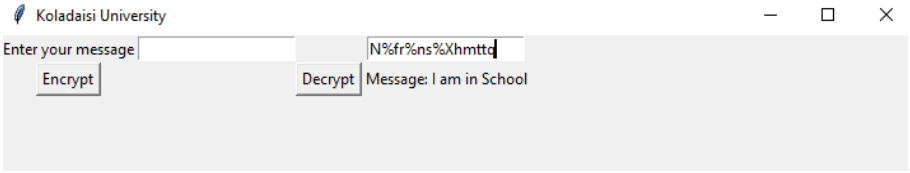

Figure 5: A Step-count Data Standard Decryption

Table 1: Evaluation of Step-Count and RSA Algorithm.

Algorithm	Message	Cipher Length	Encryption Time	Decryption Time	Message
Step-Count Model	I am in School	N%fr%ns%Xhmttq	0.00000001s	0.00000001s	I am in School
RSA	I am in School	4865904, 6684705, 2325162, 3418845, 6684705, 4865904, 5836505, 6684705, 5287343, 32104, 2156770, 299733, 299733, 259027	3.94s	3.94s	I am in School

References

[1] Zahraa, C. O., Wasan, A. A., Wisam, C. A., Ali, S. A., Liwa, H. A. (2020). Overview and Performance Analysis of Encryption Algorithm. *Journal of Physics*. https://www.researchgate.net/

[2] Santos, A., & Júnior, R. V. (2021). Improving Caesar Cipher for Greater Security. 1(9)

[3] Nurcahya, S. D., & Nazelliana, D. (2024). Message Security in Classical Cryptography Using the Vigenere Cipher Method. *International Journal Software Engineering and Computer Science* (IJSECS), 4(1), 350-357.

[4] Mays, M. H. (2020). Improved Structure of Data Encryption Standard Algorithm. *Journal of Southwest Jiaotong University*, 55(5). http://www.jsju.org/index.php/journal/article/view/723

[5] Khairul, M., and Jefril, R. (2020). Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based. *Journal of Applied Engineering and Technological Science*, 1(2). https://journal.yrpipku.com/index.php/jaets/article/view/78

[6] Pronika, S.S.(2021). Performance analysis of encryption and decryption algorithm, *Indonesian Journal of Electrical Engineering and Computer* Science, 23(2). http://ijeecs.iaescore.com