INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

ERN Cryptosystem for the Security of Textual Data based on Modified Classical Encryption Techniques

Ekta Narwal[1]*, Ritu [1], Niram[1], Deepika[2]

1 Department of Mathematics, M.D. University, Rohtak, India
2 Universitat Rovira I Virgili, Avinguda Catalunya, Tarragona

OPEN ACCESS

Received: 11-10-2022
Accepted: 22-12-2022
Published: 03-02-2023

Citation: Narwal E, R, Niram , Deepika (2023) ERN Cryptosystem for the Security of Textual Data based on Modified Classical Encryption Techniques. Indian Journal of Science and Technology 16(4): 292-298. https://doi.org/10.17485/IJST/v16i4.2009

* **Corresponding author**.

ektanarwal.math@mdurohtak.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To develop an algorithm based on classical encryption techniques that cannot be cryptanalyzed easily. **Methods:** We have proposed a new hybrid approach for the encryption and decryption of data. In this technique, some bits from the plain text, after converting it into binary form, are deleted and permuted in another place and placed back in the text. **Findings:** We examine the encryption and decryption times of various plaintexts of different sizes. Here, we compare the proposed ERN (Ekta Ritu and Niram) Cryptosystem with the algorithm based on 2's complement method based on time complexity and efficiency. **Novelty:** A table displaying the encryption and decryption times of several input files of various sizes for the proposed algorithm and the already existing algorithm is given, with a relevant graph, proves the novelty of the cryptosystem. The experimental results show that the ERN cryptosystem has better performance and efficiency than the algorithm based on 2's complement method.

Keywords: Cryptography; Data Security; Substitution; Transposition; Cipher Text

1 Introduction

The best solution to protect our data from cryptanalysis is through cryptography. As electronic connectivity has made significant progress, there is a need to secure information by cryptography. With the rapid growth of technology, encryption is the most powerful approach to strengthening security and preserving privacy. The main aim of encryption techniques is to secure the data and provide confidentiality, integrity, and authenticity [(1)]. Cryptography comes from the Greek word 'Kryptos,' which means hidden. It is the science of secret writing to keep the data secret. It plays a vital role in securing communication over the internet and provides security achieved based on the encryption techniques classified as "Private Key Cryptography, Public Key Cryptography, and Hash Function" [(2)]. Before the revolution of Public Key Cryptography, classical encryption techniques [(3)] were considered to communicate messages over an unsecured channel. These traditional encryption techniques are of two types: Substitution and Transposition.

1.1 Substitution Technique

Is one of the classical encryption techniques in which the characters present in the original text are replaced by other characters. The substitution techniques can be classified as follows: Caesar cipher[4], Monoalphabetic cipher, Polyalphabetic cipher, Play fair cipher, One-time pad, and Hill cipher[5].

1.2 Transposition Cipher

Is another classical encryption technique in which the order of alphabets in the plaintext is rearranged to form a cipher text. The bits of plain text are permuted to other places to give cipher text. The transposition techniques can be classified as follows: The Rail-Fence technique and columnar transposition cipher[5].

Using classical encryption techniques, researchers proposed various algorithms[6–8] to secure the messages over an unsecured channel. These algorithms provide security as well as confidentiality and integrity of messages. Here is a review of all the algorithms based on these techniques to make state-of-the-art cryptography. In 2015, Atish Jain et al. proposed a new algorithm to modify the Caesar cipher substitution method. He has used a randomized approach to enhance security. It used the concept of affine ciphers, transposition ciphers, and randomized substitution techniques to generate a cipher text[6]. Fahrul Ikhsan Lubis et al. (2017) presented a paper in which the encryption process was carried out three times to modify the Caesar cipher method[7]. Purnama et al. proposed a modified Caesar cipher method in which they replaced the characters into two parts: the vowels were replaced with vowels, and the consonants were replaced with consonants too. This method contains a single substitution that can easily solve by a cryptanalyst[8]. In 2022, Ritu et al. proposed an algorithm that includes a hybrid technique based on substitution cipher, transposition cipher, and 2's complement method. It uses two keys: the length of plaintext and the length of deleted bits[9].

The study and review of previous research on substitution and transposition techniques[10–13] show some security flaws when used, which shows that the resultant ciphertexts of these techniques are hackable. They cannot be applied to real-life applications, making our data and system less secure. The security flaws in the existing methods are: -

- The ciphertext is so simple that the attackers could quickly identify it.
- These existing techniques are vulnerable to brute force attacks, relative frequency, and known plain text.
- They do not attain a high level of security.
- They take more encryption and decryption time, allowing the attackers to analyze the key.

2 Methodology

2.1 Principle and Realization

The NIST defines computer security[2] as "The protection afforded to an automated information system to obtain the applicable objectives of preserving the integrity, availability, and confidentiality of information security resources." Encoding and decoding are crucial for sending secret information over an unsecured channel. These provide the security services such as confidentiality, authentication, and integrity to the messages so that cryptanalysts cannot recover the messages. By obtaining the provided key, encoding is the process through which the messages convert into an unreadable form. It is crucial for ensuring data security and safeguarding user information from unauthorized parties. Decoding the data from encrypted data into plaintext is known as decryption. Authorized individuals can only perform decryption because it needs a secret key.

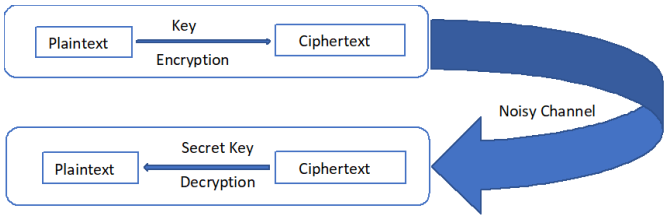
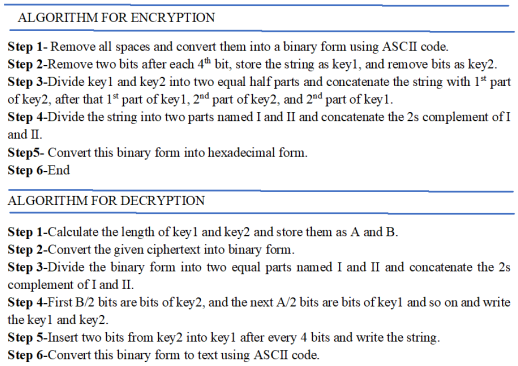


Fig 1. Block Diagram of Cryptosystem for Secure Communication

There are three basic steps to send secret information to the authorized user over a noisy channel. (1) Encrypting the plaintext into an unreadable format called ciphertext. (2) Sending the information over a noisy channel. (3) Decrypting the ciphertext to text using a secret key. These steps will provide secure communication to the users.

Figure 2 includes a hybrid technique based on classical techniques and 2's complement method [9], making the ciphertext more complex. This algorithm will take more encryption and decryption time, allowing the cryptanalysts to recover the secret key. Thus, it has a more structured ciphertext, but the time complexity is not so good.



ALGORITHM FOR ENCRYPTION

Step 1- Remove all spaces and convert them into a binary form using ASCII code.
Step 2-Remove two bits after each 4th bit, store the string as key1, and remove bits as key2.
Step 3-Divide key1 and key2 into two equal half parts and concatenate the string with 1st part of key2, after that 1st part of key1, 2nd part of key2, and 2nd part of key1.
Step 4-Divide the string into two parts named I and II and concatenate the 2s complement of I and II.
Step5- Convert this binary form into hexadecimal form.
Step 6-End

ALGORITHM FOR DECRYPTION

Step 1-Calculate the length of key1 and key2 and store them as A and B.
Step 2-Convert the given ciphertext into binary form.
Step 3-Divide the binary form into two equal parts named I and II and concatenate the 2s complement of I and II.
Step 4-First B/2 bits are bits of key2, and the next A/2 bits are bits of key1 and so on and write the key1 and key2.
Step 5-Insert two bits from key2 into key1 after every 4 bits and write the string.
Step 6-Convert this binary form to text using ASCII code.

Fig 2. Algorithm Based on 2's Complement Method

2.2 ERN Cryptosystem based on modified classical encryption techniques

This cryptosystem uses a hybrid strategy built on substitution cipher and transposition cipher to increase security and make it harder to decrypt for cryptanalysts. We are using two of the traditional encryption approaches to increase the speed and effectiveness of the encryption and decryption mechanism. This technique uses two keys, one representing the plaintext length and the other the deleted bit length. We propose this cryptosystem based on encryption methods that remove some bits from plain text and permute them in another location to increase security. This system is secure against structural attacks. The ERN Cryptosystem's encryption mechanism's flowchart is depicted in Figure 3 . We begin by using the provided plaintext in the encryption method. After performing all the steps of the encryption mechanism, we obtain ciphertext.

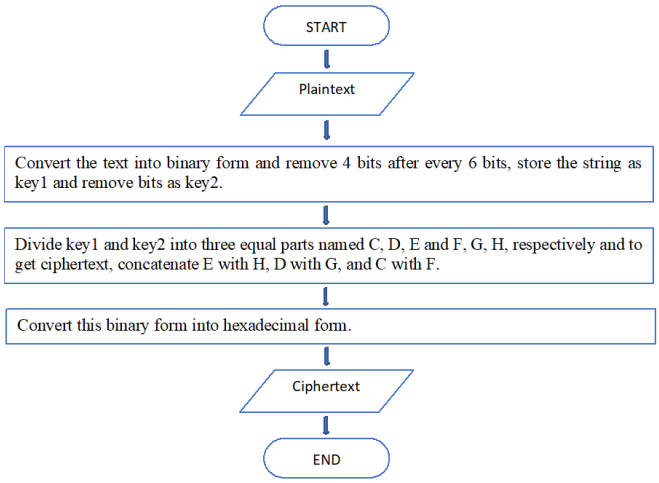


Fig 3. Flow Chart of Encryption Mechanism of ERN Cryptosystem

Figure 4 shows the decryption mechanism of the ERN Cryptosystem, in which we begin with the received ciphertext from the encryption mechanism. After performing all the steps of the decryption mechanism, we reobtained the given plaintext.

3 Results and Discussion

Example with results

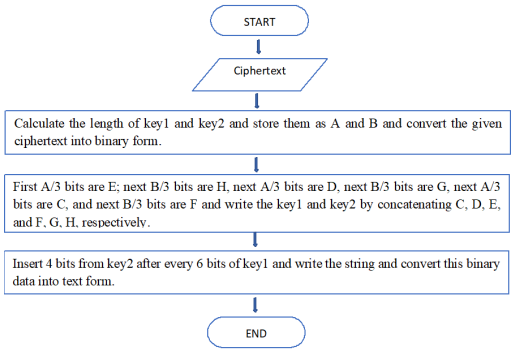


Fig 4. Flow Chart of Decryption Mechanism of ERN Cryptosystem

Encryption Process

Plain text = EVERY DAY IS A CHANGE TO BE BETTER

Step 1- Converting the text into binary form

01000101010101100100010101010100100101
10010100010001000001010110010100100 1
01010011010000010100001101001000010 0
00010100111001000111010001010101010 0
01001111010000100100010101000010010 0
01010101010001010100010001010101001 0

Step 2- Removing 4 bits after every 6 bits, storing the string as Key1 and removed bits as Key2

Key 1 = 01000101011001010110010101000 1
00000110010101010101000000001110000 1
01010001000100010101000111010001000 1
00001001010100010101010001010010
Key 2 = 01010100010010010001010100100 0
11010101000000111011010101001100100 10
10100010101000101

Step 3- Dividing Key1 and Key2 into three equal parts

C = 01000101011001010110010101000100000110010101
D = 01010100000000111000010101000100010001010100
E = 01110100010001000010010101000101010001010010
F = 01010100010010010001010100 10
G = 00110101010000001111011010101
H = 00110010010101000101010001 0
Step 4- Concatenating C with H, D with G, and E with F respectively

Concatenate = 01110100010001000010010
10100010101000101001000110010010101
00010101000101010101000000001110000
10101000100010001010100001101010100
00001110110101010100010101100101011
00101010001000001100101010101010001
001001000101010010

Step 5- Converting binary form into hexadecimal form

Ciphertext = 7444254545232545455403854445435 40ED5456565
441955449152

Step 6- End

Decryption Process

Step 1- Calculating the length of Key1 and Key2 and storing as A and B respectively
A = 132
B = 84
Step 2- Converting the ciphertext into binary form
01110100010001000010010101000101010
00101001000110010010101000101010001
01010101000000001110000101010001000
10001010100001101010100000011101101
01010100010101100101011001010100010
00001100101010101010001001001000101
010010
Step 3- First A/3 bits are E, next B/3 bits are H, next A/3 bits are D, next B/3 bits are G, next A/3 bits are C, and next B/3 bits are F respectively
C = 01000101011001010110010101000100000110010101
D = 01010100000000111000010101000100010001010100
E = 01110100010001000010010101000101010001010010
F = 0101010001001001000101010010
G = 00110101010000001111011010101
H = 00110010010101000101010010
Step 4- Writing the Key 1 and Key 2 by concatenating C, D, E and F, G, H respectively
Key 1 = 01000101011001010110010101000
01000001100101010101010000000001110
00010101000100010001010100011101000
01000100001001010100010101000101000
10
Key 2 = 0101010001001001000101010010
00011010101000000011101101010100110
0100101010001010100010
Step 6- Inserting 4 bits from Key 2 after every 6 bits of Key 1 and writing the string by converting it into text form
Decrypted Text = EVERYDAYISACHANGETOBEBETTER
Step 7- End

Here, we have taken EVERY DAY IS A CHANGE TO BE BETTER as plaintext. On applying various steps of the encryption process to the given plaintext, we obtain ciphertext as 7444254545232545455403854445435540ED5456565441955449152. After using various steps of the decryption process to the received ciphertext, we have reobtained the plaintext: EVERY DAY IS A CHANGE TO BE BETTER.

3.1 Performance analysis of ERN Cryptosystem

This section focuses on the time complexity and efficiency of the ERN Cryptosystem, as given before, and compares it with the algorithm based on 2's complement method [9]. In both algorithms, some bits are initially deleted from the original string and permuted to other places. Here, we count the encoding and decoding time of the ERN cryptosystem and algorithm based on 2's complement method. The software we used is MATLAB 2021, running on the 64-bit Windows11 operating system, and the hardware parameters are Intel Corei5-1135G7,2.42GHz, 8 GB RAM.

Table 1 shows the time of different plain texts taken for encoding and decoding (in seconds) for the proposed cryptosystem and algorithm based on 2's complement method. Figure 5 shows the relevant graph of the comparison table.

The Encoding and Decoding time taken by the ERN Cryptosystem and algorithm based on 2's complement method for five different size input files is depicted in Figure 5 graphically for analysis. By analyzing Table 1 and Figure 5 we can say that the Encryption and Decryption time taken by the proposed cryptosystem is less than that based on 2's complement method. An algorithm based on 2's complement method has taken more time for encryption and decryption. However, the algorithm's complexity is more based on 2's complement method. According to the experimental findings, the ERN cryptosystem performs better and is more effective than the 2's complement-based algorithm.

Table 1. Encoding and Decoding Time for ERN Cryptosystem and algorithm based on 2's complementmethod

Iteration	File Size (In bits)	ERN Cryptosystem (Encoding and Decoding time in seconds)	An algorithm based on 2's complement method (Encoding and Decoding time in seconds)
1	96	0.077	0.091
2	184	0.082	0.111
3	216	0.084	0.114
4	336	0.088	0.136
5	360	0.095	0.138

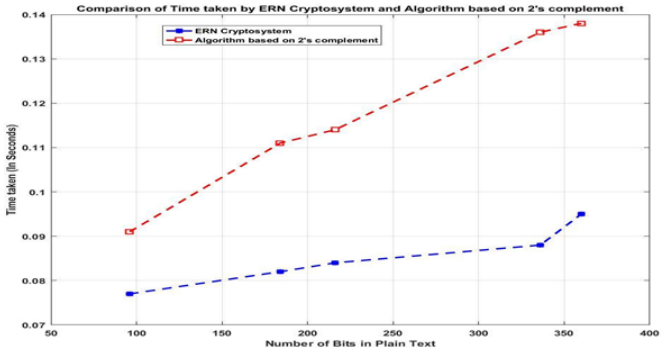


Fig 5. Encoding and Decoding Time for ERN Cryptosystem and Algorithm Based on 2's Complement Method

4 Conclusion

This study has proposed a hybrid technique for encryption and decryption using classical encryption techniques. In this technique, we have secured the data by making ciphertext stronger than the existing algorithms. We examine the encryption and decryption times of various plaintexts of various sizes and compare the proposed ERN Cryptosystem with an algorithm based on 2's complement method. A comparison table of encoding and decoding time of both the algorithms and the relevant graph of the comparison table is given. The experimental analysis shows that the proposed cryptosystem has better performance and efficiency than the algorithm based on 2's complement method. It can be used for any variable length of the text and resists brute force and relative frequency attacks. Thus, this technique is secure and efficient and can be implemented for low-scale purposes. This cryptosystem is valid only for textual data. In the future, we will improve our cryptosystem by encrypting both image and textual data using permutation techniques.

Acknowledgment

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-public sectors.

References

1) Bhargava U, Sharma A, Chawla R, Thakral P. A new algorithm combining substitution & transposition cipher techniques for secure communication. *2017 International Conference on Trends in Electronics and Informatics (ICEI)*. 2017. Available from: https://doi.org/10.1109/ICOEI.2017.8300777.
2) Stallings W. Cryptography and Network Security Principles and Practices. Pearson/Prentice Hall. 2009. Available from: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptographyand-network-security_-principles-and-practice-7th-global-edition.pdf.
3) Majumder R, Datta S, Roy M. An Enhanced Cryptosystem Based on Modified Classical Ciphers. *8th International Conference on Advanced Computing and Communication Systems (ICACCS)*. 2022;p. 692–696. Available from: https://doi.org/10.1109/ICACCS54159.2022.9785033.
4) Masud KI, Hasan MR, Hoque MM, Nath UD, Rahman MO. A New Approach of Cryptography for Data Encryption and Decryption. *5th International Conference on Computing and Informatics (ICCI)*. 2022;p. 234–239. Available from: https://doi.org/10.1109/ICCI54321.2022.9756078.
5) Qadir AM, Varol N. A Review Paper on Cryptography. *7th International Symposium on Digital Forensics and Security (ISDFS)*. 2019. Available from: https://doi.org/10.1109/ISDFS.2019.8757514.
6) Jain A, Dedhia R, Patil A. Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. *International Journal of Computer Applications*. 2015;129(13):6–11. Available from: https://doi.org/10.48550/arXiv.1512.05483.

7) Lubis FI, Simbolon HFS, Batubara TP, Sembiring RW. Combination of Caesar Cipher Modification with Transposition Cipher. *Advances in Science, Technology and Engineering Systems Journal*. 2017;2(5):22–25. Available from: https://doi.org/10.25046/aj020504.
8) Purnama B, Rohayani AHH. A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from a Message to Be Encrypted. *Procedia Computer Science*. 2015;59:195–204. Available from: https://doi.org/10.1016/j.procs.2015.07.552.
9) Ritu N, Narwal E, Gill S. A Novel Cipher Technique Using Substitution and Transposition Methods. In: Rising Threats in Expert Applications and Solutions. *Lecture Notes in Networks and Systems*. 2022;p. 123–129. Available from: https://doi.org/10.1007/978-981-19-1122-4_14.
10) Renuka K, Harshini GN. Analysis and Comparison of Substitution and Transposition Cipher. *IJRAR- International Journal of Research and Analytical Reviews*. 2019;6(2):549–555. Available from: http://ijrar.com/upload_issue/ijrar_issue_20543567.pdf.
11) Brezočnik L, Fister I, Podgorelec V. Nature-Inspired Cryptoanalysis Methods for Breaking Vigenère Cipher. In: New Technologies, Development and Application III. Springer International Publishing. 2020;p. 446–453. Available from: https://www.iztok-jr-fister.eu/static/publications/268.pdf.
12) Saboncchi AKS, Akay B. A binomial crossover based artificial bee colony algorithm for cryptanalysis of polyalphabetic cipher. 2020. Available from: https://doi.org/10.17559/TV-20190422225110.
13) Wulandari GS, Rismawan W, Saadah S. Differential evolution for the cryptanalysis of transposition cipher. In: 2015 3rd International Conference on Information and Communication Technology (ICoICT). IEEE. 2015;p. 45–48. Available from: https://doi.org/10.1109/ICOICT.2015.7231394.