Eximia Journal

(ISSN 2784-0735)

Vol. 9

2023

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

Proposed Method for Efficient Block Cipher Cryptography

Amina Khaled Khalel Alregabo[1]

Amina.20csp64@student.uomosul.edu.iq

Yassen Hikmat Ismail[1]

yaseen-hikmat@uomosul.edu.iq

[1]Computer Science Department, University of Mosul

Abstract. After the use of the Internet and the transmission of files between users expanded, information security became one of the important priorities for securing information by different means and methods. The information encryption comes at the forefront of the techniques used in information security. Encryption has been known since ancient ages. So, traditional methods appeared that quickly and greatly developed. They are still used in many scientific studies and developmental research with the aim of developing new methods for encryption of substitutions and increasing its ability to confront various attacks. The traditional methods were subjected to several attacks that they prompted researchers to develop them and overcome their weaknesses in front of those attacks. Some combinations of these methods are used to design new encryption methods based on overlapping ideas of traditional encryption. This paper sought to use a set of traditional encryption methods in designing a new system. In which, these methods are mixed with modern ideas that help increase the strength of encryption and its ability to face potential attacks. Caesar, Vigenère, Rail Fence, and transpose ciphers, with the idea of cipher cycles and segments and division into two parts in block ciphers. The proposed system relied on the chaotic function Tent map for its random properties in generating a string of keys consisting of 112 random characters in length using Python 3.11 programming language. The text was cut into Blocks of 108 characters. Each Block was divided into two parts. A part of the key was added to each section. A rial fence method was applied. Then Vigenère method with the key is applied. The proposed system processed the original text within the framework of the encryption cycles with the use of substitution in the order of the columns, shifting to the right, and the replacement of the sequence of the elements of each side according to the order of the elements of the other side. After the end of the encrypting cycles, the cipher block is added to the final ciphertext. The operations were repeated for the next block until the last block is finished. For the purpose of decrypting, the previous operations are repeated in reverse order to obtain the original text, by decrypting blocks of the cipher text. The proposed system achieved extreme accuracy in extracting the original text. The system was evaluated by measuring the time and throughput of the encryption and decryption. The encryption and decryption times were short for short texts, which increased with the increase in the length of the text, with a relatively stable encryption and decryption throughput. The system achieved acceptable memory consumption in short texts but increased by the length of the text size. The achieved Avalanche test was less than (50%).

Keywords. Block cipher, Chaotic map, Tent map, Cesar Cipher, Rail fence, Vigenère.

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

1. Introduction

Today, the world is witnessing the era of information technology, and a wide spread of innovative and developed applications on the Internet, as the process of exchanging information has become accessible to everyone and easy to use, and it has become necessary to rely on an effective method to protect data transmitted via the Internet, to prevent unauthorized persons from accessing it[1]. The researchers presented many encryption systems to enhance the security of networks and applications over the Internet, and used block encryption methods as one of the important encryption systems that can achieve data security, and developed many algorithms based on the main principles of Block Ciphers, and presented many ideas and modifications. Which includes improving these algorithms to reach higher performance and strength of encryption systems [2].

Presenting a large number of encryption systems of different types requires performance analysis to evaluate the quality of the performance of these methods, as the analysis allows the researcher to monitor the weaknesses of previous algorithms against attacks and develop them by building new and more powerful algorithms [3]. Among these algorithms, block ciphers play a major role in many network applications. Several block cipher algorithms have been introduced to increase their performance level and strengthen their capabilities against attack[4]. Data encryption is a security solution, which converts normal data into encrypted data in the encryption stage, while the reverse process is called decryption, which converts encrypted data into normal data, and encryption algorithms usually aim to recover the original data after the decryption stage without losing any part in The recovered data, and the robustness of the algorithms against different types of attacks is very essential, to secure the data sent over any communication medium [5]. The encryption methods based on the replacement of letters are traditional methods that have witnessed many updates and modifications, so their strength and security have developed, and they have been used to protect and secure data. Encryption (Rahim & Ikhwan, 2016). Although the old methods of character-based encryption were weak due to the repetitions of those characters in natural language, the modifications made to them made them able to face many types of attacks to break their code or access the encryption keys[6].

2. Literature Review

Many researchers presented many solutions to develop block cipher based on texts with letters. Their contributions added great benefit in developing encryption systems, and the most important of these works are :

(Hasani, 2023 & Shareef) presented an encryption method based on matrix transposition technology to develop the matrix-based encryption method. The use of matrix transposition in the encryption method enhanced the secrecy and complexity of the method. The researchers put the plain text in a two-dimensional matrix, then changed the order of the columns in the matrix is according to the numbers of the encryption key. This method added a kind of complexity to the encryption process that makes the traditional methods more capable of facing cryptanalysis[7]. (Thakkar & Thankachan, 2021) used multi-level technology using two switching techniques, which are rail fence encryption and simple vertical encryption. This method aims to enhance the level of security, with plain text encrypted using Rail Fence encryption technology. The cipher text is passed as a plain text message to the simple vertical encryption technique, resulting in the final ciphertext. This method achieved a higher level of security than using the methods used separately[8]. (Shruthy & Veerasamy, 2021) proposed a hybrid approach to encoding the plain text using Playfair Cipher and Simple Columnar Transposition. The researchers adopted two different tagging methods; They are the simple sequential extra tags, and the tags on the second space of some graphs associated with the tree diagram resulting from the encryption process. This method contributed to increasing the complexity in the face of code analysis [9]. (Bitar & Sujatha, 2021) presented the hybrid "Railve" algorithm, which consists of merging the standard traditional encryption algorithms "Vernam Cipher" and "Rail-Fence Stream". The resulting algorithm was characterized by high performance. It consumes a small amount of RAM. By applying the three algorithms on two devices “a mobile phone and a laptop”, the results after integrating the Vernam algorithm with the RailFence algorithm showed good results, more security and less ciphertext size compared to the

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

original encryption algorithms [10]. (Toull et al. 2020) presented a hybrid of Vigenere and Hill ciphers belonging to the block cipher family, by exploiting the previous improvements by implementing Hill cipher to hide the weakness of the Vigenere algorithm, which is the ease of detecting the key size to initiate a statistical attack, as well as the weakness of the cipher algorithm. It has two consecutive similar characters in different blocks. The results showed the coherence between these two methods that created a reliable hybrid algorithm, with resistance to various attacks, including statistical attacks[11]. (Nahar & Chakraborty, 2020) presented a technique for organizing the plain text transversely in the Rail Fence method, so that reading it from the upper row to the lower row leads to the production of the ciphertext. The researchers redesigned the standard Rail Fence application The three basic stages: the replacement stage once, and the transfer stages are used twice. The proposed technique ensures that the resulting ciphertext is an amalgamation of different symbols precisely defined by the scheme. The proposed algorithm eliminates the limitations of the standard algorithm, and significantly improves performance by converting plaintext into ciphertext, which is unrecognizable and unpredictable [12].

3. Block Cipher

It is one of the types of symmetric encryption that depends on a single key in the encryption and decryption processes. Methods of this type divide the plain original text into blocks, which are encrypted using the key for each block, and the ciphertext is divided into the same blocks that are decrypted using the key itself, and this type of encryption is widespread due to its low cost and sufficient protection for the encrypted information, but it falls short of achieving very high encryption strength[13].

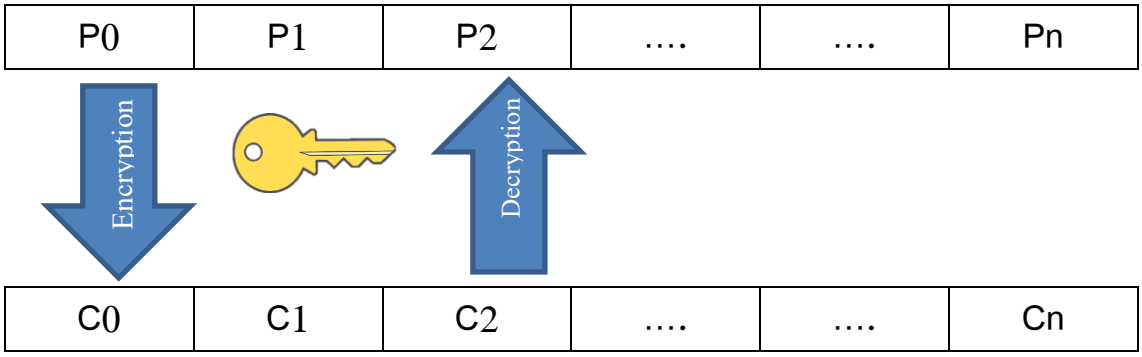


Figure 2: Block cipher

In the previous figure, we notice that each section of the original text is encrypted using the key, and the encrypted text is decrypted using the same key for each section separately as well.

3.1. Key Generation

Symmetric or asymmetric encryption systems rely on keys to encrypt the original data and convert them into ciphertexts or to decrypt the encrypted data and return it to the original texts. The strength of the encryption system depends on the strength of the key used. and unbreakable [14].

Several functions are used to generate the key, including the Pseudo Random Number Generators (PRNGs) function, which is a deterministic algorithm that uses mathematical operations to generate keys, but random numbers and their frequency can be predicted using this function[15]and researchers began to introduce other methods to generate more robust and random keys using fingerprint[16] or voice[17], or using chaotic Maps[18]. The use of two or more types of key generation functions to increase

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

strength and randomness in the face of various attacks[19, 20] and in order to obtain random keys, the length of the key chain must be appropriate to the encryption method, so it is not Vulnerable to statistical attacks targeting key length, especially keys with short strings.

The properties of chaotic maps contribute effectively to achieving the randomness used in generating the key used to encrypt the data. Chaotic maps can be classified into continuous and discrete, as follows:

A) Continuous chaos functions

A type of chaotic maps in which chaotic continuous systems are simulated on analog circuits, and can be modeled using ordinary differential equations. are representative signals (Alawida et al., 2019). An example of continuous chaotic maps represented by integers and in three dimensions is Chua circuit[21], Duffing equation [22], Finance system [23].

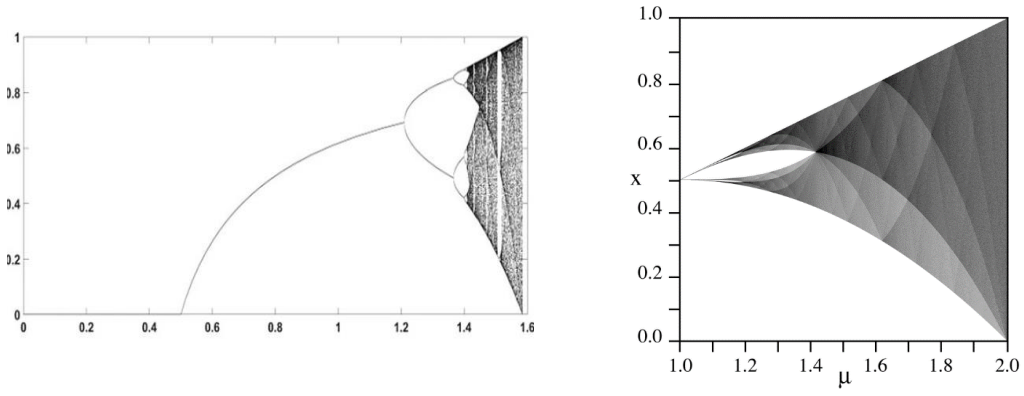
B) Discrete Chaos Functions

Definition 1: The iterative discrete function in one dimension is defined as a function of the form (1):

$$x(k+1)=f(x(k),\alpha) \quad \dots (1)$$

where: $x \in C$ is a quantitative measure, f is a nonlinear analytical function, and $\alpha \in C$ represents the coefficients of the vector. A function is considered chaotic if x belongs to the complex set representing chaotic behavior [24].

The researchers introduced several discrete chaotic functions in order to enhance the properties of chaotic behavior that are used as key generation functions in cryptography, such as Arnold's cat map[25], Circle map[26], and Complex squaring map[27], the Exponential map [28], and the Tent map[29]. Figure (3) shows the representation of the Temp map.



a) Exponential map b) Tent map

Figure 3:Temp map and Exponential map.

Chaotic maps, especially discrete chaotic map, make up the most efficient key generation function, whether used alone or in combination with different functions or data sets. The encryption key must be unpredictable and very sensitive to very small changes in its value. This is why chaos maps are so important. Because they have properties that enable to generate random numbers such as bifurcation, unpredictability, and sensitivity to initial conditions[30].

3.2. 4 Block Cipher Modes

Block cipher operating modes are techniques that used to enhance the effect of the cryptographic algorithms, or to adjust the algorithms for applications. There are five operating modes to be used in these technologies:

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

A) Electronic Codebook (ECB):

Each block of 64-bit plain text is encoded independently using the same key. It is the easiest of the rest of the patterns, but it is the weakest due to the lack of auditing technology for the accuracy of the encoded data. This mode is often used for the secure transfer of individual values (e.g.; an encryption key)[31] (Abdullah H., 2016).

B) Cipher Block Chaining (CBC):

The input of the cipher algorithm is an XOR result of the next 64 bits of the plaintext and the previous 64 bits of the previous ciphertext. Finding plaintext in a specific block requires knowing the current ciphertext, the key, and the ciphertext of the previous block. When an error occurs, the error moves to the next blocks, which is more secure than the previous mode. This mode is used for general transmission purposes and reliability [34].

C) Cipher Feedback (CFB):

Its input is being processed bits at a time, the previous ciphertext is used as input for the cipher algorithm to produce a pseudo-random output, which is XORed with plaintext to produce the next unit of ciphertext. It has the ability to add additional bits at the end of the block that is less than 64 bits in size, and this mode is used for general transmission purposes. Reliability [34].

D) Output Feedback (OFB):

Similar to CFB, except that the input of the cryptographic algorithm is the output of the previous ciphered block. The full blocks are used. It has the ability to add extra bits at the end of a block of size less than 64 bits, and detect it from the receiving end, but it is less secure than the previous mode. This mode is used in directed transmission of the stream over a download channel (for example, satellite communication) [34].

E) Counter (CTR):

Each plaintext block is XORed with the encoder's counter. The counter is incremented for each subsequent block. This mode is used in a general-purpose geared transmission that is useful for high-speed requirements [34].

4. The proposed System

The design of the proposed system is based on integrating a set of ideas inspired by the traditional encryption methods incorporated in Feistel's design to encrypt and decrypt a 108-character block of the original text using a key of 112 characters in length, during 8 cycles. The proposed encryption system consists of two basic phases, like other encryption systems, They are the encryption phase and the decryption phase, as follows:

4.2.1 Encryption phase

The encryption phase begins with the process of generating the key that depends on the Tent Map function defined in the program, to obtain a string of highly random numbers, which is converted into the corresponding letters using mathematical functions and based on the American Standard Code for Information Interchange (ASCII) of the English letters used in the original text. According to equation (2).

$$K_i = R_i \% 26 + 65 \ldots (2)$$

where:

K: represents the key

R: represents the random number string.

Applying the previous model produces a series of numbers associated with the letters of the alphabet, which will be used as a key for encryption or decryption.

After completing the key generation process, the encryption steps begin. The original text is divided into a specified number of syllables, which are commensurate with the design of the proposed system, by applying equation (3):

$$\text{Block count} = \text{Length}(P) / \text{length (block)} \ldots (3)$$

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

where:
Block count: The number of blocks to be encoded.
Length(P): The length of the original text, P.
length (block): The length or size of the block, equal to 108, according to the proposed design.
Often the length of the original text does not agree with the length or size of the blocks, so the resulting fraction is forced into the next integer, and the amount required to complete the last syllable is added by part of the first syllable. As in (Figure 4).

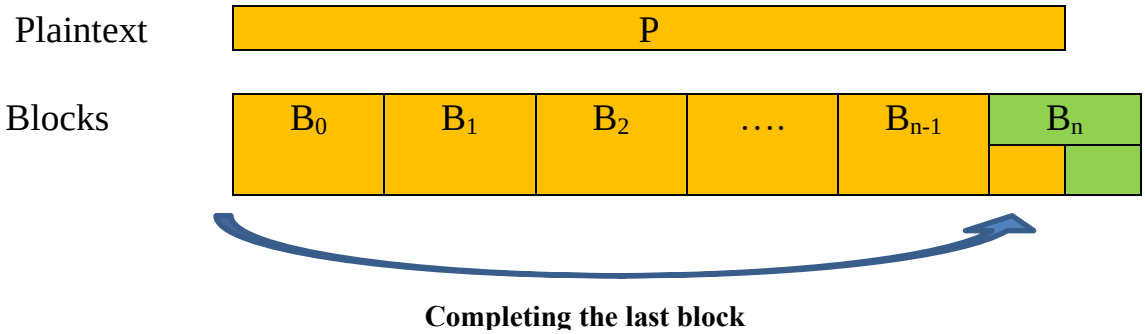


Figure (4) Division of the original text with algebra of the last syllable.

The third step of the encryption steps is to divide the text according to Feistel's design for block cipher systems, so the original text is divided into two parts, both of which have a size of 54 characters. In (Figure 5).

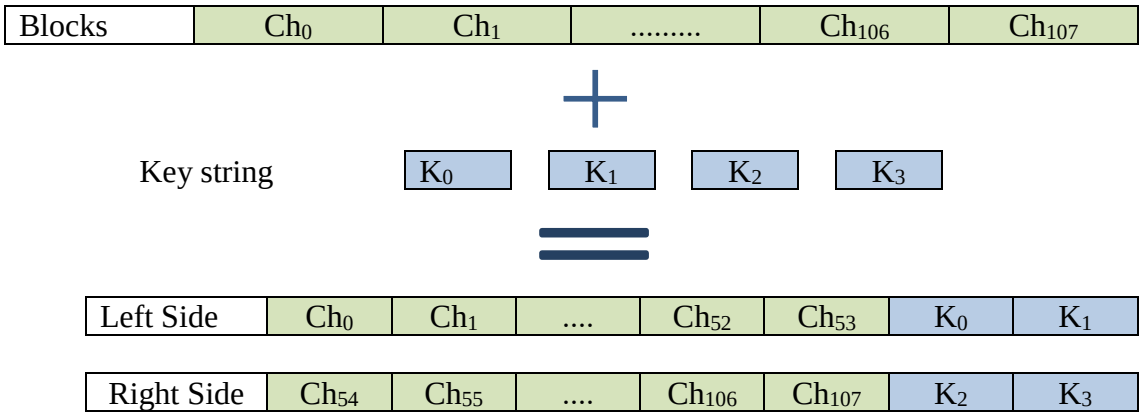


Figure 5: Dividing the syllable into two parts, adding two letters of the key to them.

The fourth step begins with applying the railway fence algorithm, with a depth of (Depth = 2), for both the right and left sections, so the output will be two matrices (2×28), and this step contributes to increasing the spread, as shown in (Figure 6).

Left Side	Ch_0	Ch_2	....	Ch_{52}	Ch_{54}
	Ch_1	Ch_3	....	Ch_{53}	Ch_{55}

Right Side	Ch_{56}	Ch_{58}	....	Ch_{108}	Ch_{110}
	Ch_{57}	Ch_{59}	....	Ch_{109}	Ch_{111}

Figure 6: Application of the rail fence algorithm

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

The fifth step begins with applying the Vigenère method, which forms a matrix for each section with dimensions (7 lines x 8 columns), with adding the key for each element of the two sections, as shown in (Figure 7).

Left side K(0-55)

L_0	L_1	-	-	-	-	L_6	L_7
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
L_{48}	L_{49}	-	-	-	-	L_{54}	L_{55}

Right side $K_{(56-111)}$

R_0	R_1	-	-	-	-	R_6	R_7
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
R_{48}	R_{49}	-	-	-	-	R_{54}	R_{55}

Figure 7: Application of the Vigenere method.

The previous steps prepared the original text and converted it into a two-dimensional matrix in both sections with encryption using the key in the previous step, after which the encryption cycles adopted in the block cipher begin, and depending on the size of this matrix, the number of encryption cycles was 8 cycles that ensure complete calibration in the elements of the original text, and the addition of More confusion and spread.

The sixth step begins within the encryption cycles, which is the process of switching the positions of the columns from the Columnar Transpose encryption method, so the columns are replaced in both the right and left sections based on the order of the key letters, and the key part (0-7) is used for the left section, and (8-15) for the right section, For example, when the key is ('Q', 'P', 'W', 'H', 'Y', 'X', 'J', 'O'), the order of the columns is in the order of letters as shown in the table (1).

Table 1. Extracting the order of the columns from the key.

Style	Example and use
Part of the key	'Q', 'P', 'W', 'H', 'Y', 'X', 'J', 'O'
Ascending Order	'H', 'J', 'O', 'P',' Q', 'W', 'X', 'Y'
Corresponding order	[4, 3, 5, 0, 7, 6, 1, 2]

The seventh step transforms the positions of elements in the left and right sections, using the idea of Transpose cipher, in which the elements of the two sections are arranged, so the elements of the right section are arranged horizontally, starting from the bottom right, while the elements of the left section are arranged vertically from the top left.

The eighth step replaces the fifth column L4 from the left section with the second column R1 from the right section, and the fifth column R4 from the right section with the second column L1 from the left section, which is a switching process between the two sections that results in a change in the order of their elements, and thus the general arrangement of the ciphertext. In order to increase the complexity, the ninth step rotates the columns of the two sections once to the right.

In the tenth step, the matrix format is changed from 7 lines and 8 columns to 8 lines and 7 columns.

The eleventh step comes by changing the order of the elements of some columns in both sections depending on the other section, by fixing the first column RC0 and the third column RC2 for the right section to use their arrangement in changing the order of the first column LC0 and the third column LC2 from the left section, and on the other hand, by installing the second column LC1 And the fourth column LC3 of the left section to use their order in changing the order of the second column RC1 and the fourth column RC3 of the right section, and for the purpose of arranging the letters a function was relied on to extract the order of the letters in the fixed columns of both sides to change the order of the variable

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

columns on the other side. At the end of this step, steps from the sixth to the eleventh are repeated for seven more times, to complete the eight cycles.

After completing the eight cycles, the two sections are encrypted with the key using the Caesar method. By replacing the characters of the text by shifting the characters by the amount of the key, and obtaining the text encrypted with the key. The elements of the left and right sections are encrypted with a shift by the amount of the key letters. In the final step, convert the two sections into a linear array, swap the two sections into each other, and combine them together to form the final ciphertext.

Figure 8 shows the flowchart that includes the operations in the steps that were previously explained, and explains the method of encoding cycles and dividing the original text into segments according to the principle of block encryption.

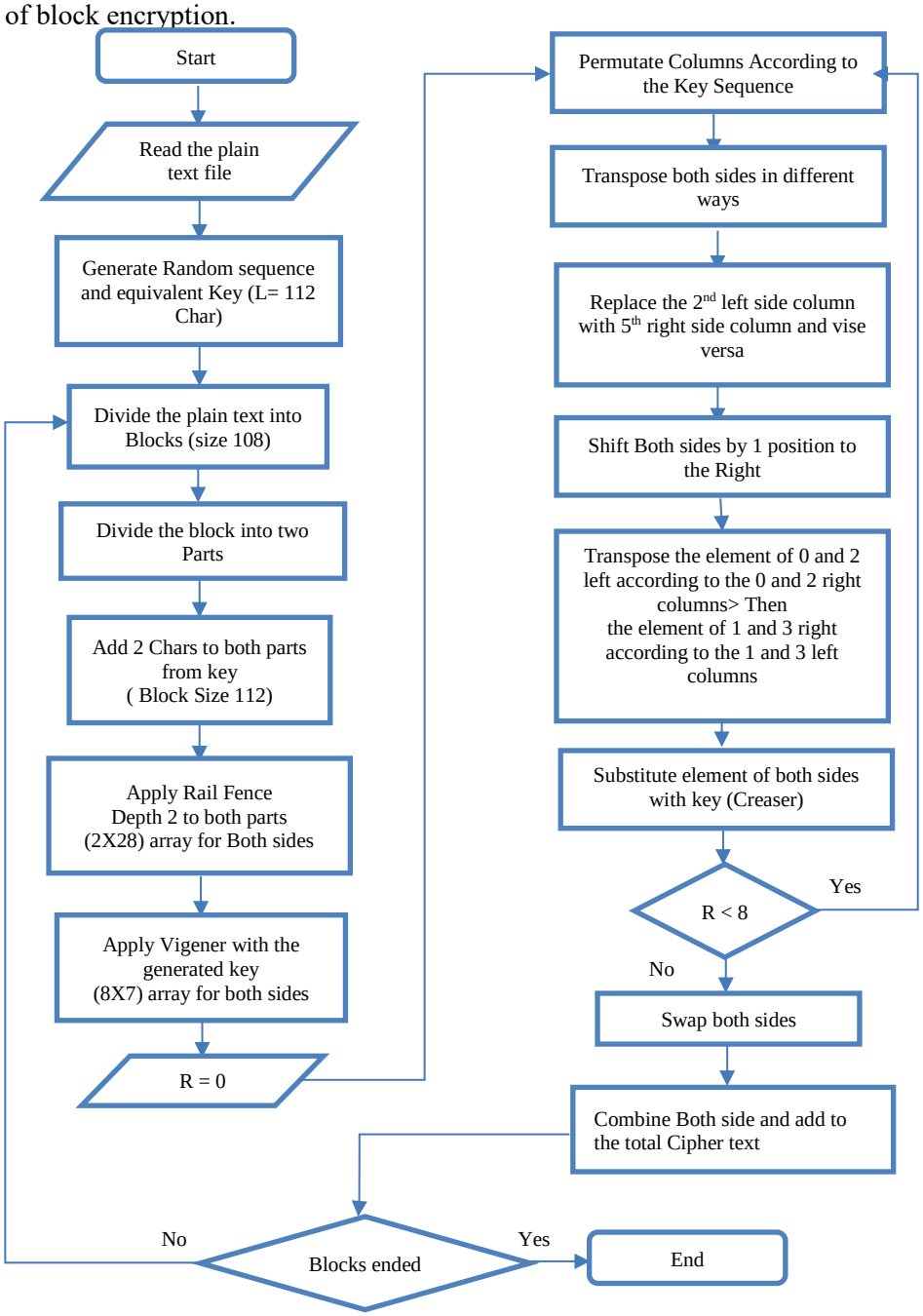


Figure 8: Flowchart of the encryption process in the proposed system.

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

4.2.2 Decryption phase

When encrypting any text, decryption must be performed to restore the original text. In the proposed method, the decryption procedure requires reverse steps to the encryption steps, as follows:

The first step starts with splitting the ciphertext into two parts based on the last step of the encryption process, the right part being swapped for the left. The second step is to reverse-shift the letters as far as the key letters. It begins with the third step with the reverse cycles of decoding, in which the encryption steps are applied in reverse, and begins by changing the shape of the matrices from linear form to 8 lines and 7 columns.

This is followed by changing the order of the elements of some columns in both sections depending on the other section, by fixing the first column RC0 and the third column RC2 of the right section to use their arrangement in changing the order of the first column LC0 and the third column LC2 of the left section, and on the other hand, by installing the second column LC1 and column The fourth LC3 for the left section to use their arrangement to change the order of the second column RC1 and the fourth column RC3 from the right section, and for the purpose of arranging the letters a function was relied on to extract the order of the letters in the fixed columns of both sides in the arrangement of the variable columns on the other side, by extracting the ascending order of the fixed column, and the column order variable in the new order. The fourth step is to change the shape of the matrix from 8 lines and 7 columns to 7 lines and 8 columns. The fifth step rotates the columns of the two sections once towards the left.

The sixth step replaces the fifth column L4 from the left section with the second column R1 from the right section, and the fifth column R4 from the right section with the second column L1 from the left section. The seventh step converts the locations of elements in the left and right sections, using the idea of Transpose cipher to arrange the elements of the two sections, so the elements of the right section are arranged horizontally starting from the left by taking the elements from the bottom right horizontally, and the elements of the left section are arranged horizontally starting from the top left.

The eighth step begins with the process of switching the positions of the columns using the Columnar Transpose encryption method. The columns are swapped in both the left and right sections based on the ascending sequence of the key letters. The key part (0-7) is used for the left section, and (8-15) for the right section. The first column is the sequence whose value is (0), and so on for all columns. After this step, steps from the third to the eighth step are repeated seven times to complete the decoding cycles.

After the end of the eight decryption cycles, the ninth step reverses Vigener's method, subtracts the key from the left and right parts, and reconfigures the two matrices from (7 lines x 8 columns) to (2 x 28), for both sections. The tenth step begins with the reverse application of the railway fence algorithm, with a depth of (Depth = 2), for both the left and right sections, so the result is two matrices (1 x 56). In the eleventh step, the key fragment is cut from both parts, and joined together to form the original text of the current fragment in reverse of the fragmentation in Feistel's design of block cipher systems. After completing the decoding of the first segment, the algorithm is repeated to decode the rest of the segments until the encrypted segments are finished. Figure 9 shows the flowchart of the decoding process in the proposed system, the method of reverse processing of the ciphertext and extraction of the original text, passing through the decoding cycles and other operations in their reverse order.

5. The Results

The method was applied to encrypt 12 files containing the original text, by generating the encryption key based on Ten map, 112 characters long, and the original text was divided into segments, the size of each segment is 108 characters, and the last text segments were completed for the purpose of completing the encryption process.

5.1 Results of encryption and decryption

The encryption process was carried out according to the proposed method and with all eight encryption cycles for all files, and the results of the encryption process showed a complete change to the original text, resulting in a completely encrypted text, no similarity remains between the original text and the encrypted text in all files, and this indicates the spread achieved by the encryption method.

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

The method was applied to decrypt 12 files containing the ciphertext, using the encryption key saved for each previous process The decryption results were completely identical to the plaintexts in all files.

This is an indication of the accuracy of the work in designing the reverse performance of the proposed method.

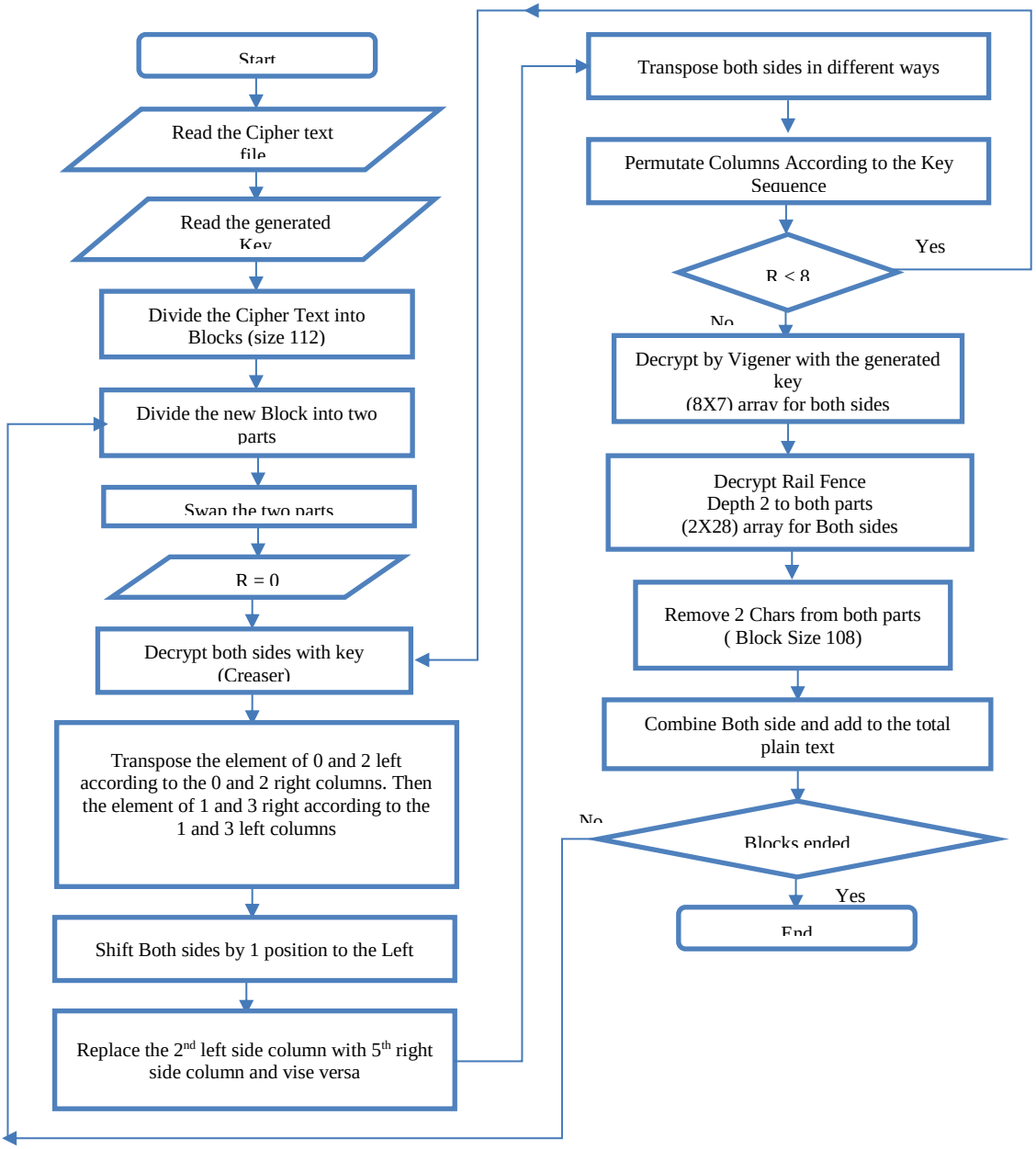


Figure 9: Flowchart of the decryption process in the proposed system.

5.1 Text Recovery Results

The intelligent method of recovering the text in separate parts was applied to the output of the decryption process for all text files that contain the ciphertext, and the results of the recovery were high performance, during which the parts of the text were separated after decoding completely identical to the original text.

5.2 Performance Measures

After applying the proposed method in encoding and decoding, the results of the performance evaluation criteria were collected, which show the strength of the proposed method, as follows:

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

A- Randomness of the Key

At each new encryption process, an encryption key based on the Tent map is generated, and key generation is one of the most important challenges in the design of encryption methods in general. NIST are used to evaluate the random ness if the key. The results illustrated as follow in Table 2.

Table 2: Result of Randomness by NIST.

Test	P value	Result	Test	P value	Result
Frequency Test (Monobit)	0.830324257656	Random	Maurer's Universal Statistical test	-1.0	Non- Random
Frequency Test within a Block	0.8469215244891	Random	Linear Complexity Test	-1.0	Non- Random
Run Test	0.00015212412199	Non- Random	Serial test	0.053655284074871	Random
Longest Run of Ones in a Block	0.00708830029097	Non- Random	Approximate Entropy Test	1.0	Random
Binary Matrix Rank Test	-1.0	Non- Random	Cumulative Sums (Forward) Test		Random
Discrete Fourier Transform (Spectral) Test	0.001653656165352	Non- Random	Cumulative Sums (Reverse) Test		Random
Non-Overlapping Template Matching Test	0.995110396166	Random	Random Excursions Test	0.75784684754181	Random
Overlapping Template Matching Test	Nan	Non- Random	Maurer's Universal Statistical test	0.43762744413604	Random

Most of the randomness tests showed that the generated key is random. Tis indicates to the efficiency of key generation.

B- Key space

The length of the used key is 112 characters, and it is a long key that has the ability to face attacks on short keys, and each letter is compensated by (P=26) case, so the key space is according to equation (4):

$$Key\ space = keyLength^{p} = 26^{112} \ldots (4)$$

The key space is (2.9992 × 10 158), which is a large space whose probabilities are not easily predicted.

C- Memory consumption

The Tracemalloc library was used to measure the amount of memory consumed in encoding and decoding operations. Table (3) and Figure (10) show the results of evaluating memory consumption according to the sizes of encrypted files.

Table 3: Memory consumption in encryption and decryption.

No	File size	Consumption of encryption	Consumption of decryption
1.	1 KB	52668	51110
2.	2 KB	83870	224614
3.	8 KB	254728	1040702
4.	8 KB	257519	1055197
5.	15 KB	477757	2003457
6.	33 KB	1007918	4537971
7.	328 KB	9940579	45093870

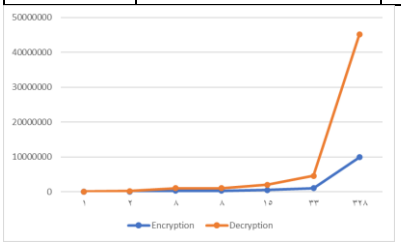


Figure 10: Memory consumption in encryption and decryption.

Eximia Journal
Vol. 9, 11-24, May, 2023
ISSN: 2784-0735
www.eximiajournal.com

It is noticeable in Figure (10) that the memory consumption in the decryption process is higher than in the encoding process, meaning that the decryption process needs more memory than that needed by the encoding process.
It is noted that the memory consumed in the proposed system increases with increasing file sizes, and increases almost linearly with increasing file size, and this indicates that the encryption method is more effective in terms of memory consumption when used with smaller files.

D- Encryption and decryption time

The time required for encryption and decryption were measured from the start of the key generation process until the end of the encryption process with its specified cycles. The times spent in the encryption process were recorded according to the sizes of the encrypted files. Table (4) show the results.

Table (4) Encryption process time.

No.	Files Size	Encryption Time	Decryption Time
1.	1 KB	0.104012	0.106998
2.	2 KB	1.124996	1.181998
3.	8 KB	5.716289	6.151922
4.	8 KB	5.837646	6.308717
5.	15 KB	11.226301	11.994603
6.	33 KB	25.571091	27.452200
7.	328 KB	261.713463	283.770056

It is noted in the encryption and decryption process that the required time increases with the increase in the size of the encrypted text file. The increase is almost linear according to Table (4), which indicates the efficiency of speed of the proposed cipher with smaller sizes.

6. Conclusion

Encryption is one of the basic issues in information security, and traditional encryption is one of the foundations on which modern encryption methods are built and are still used to preserve important data.

The key space used in the process of breaking the encryption key was large enough to make the proposed system able to face attacks on the key. The use of chaos functions positively affects the randomness of the generated key in the proposed system, which makes predicting the key a difficult process. The proposed system achieved very short encoding and decoding times with small text files, and the time increases with increasing the sizes of those files. The proposed system achieved serious productivity in the encoding process, which starts to increase with the increase in size in small text files, and stabilizes after the files start to increase in size. The proposed system achieved good decoding productivity with files of small sizes, however, the decoding productivity begins with a rapid decrease with a large increase in file size. The proposed system achieved an increased consumption of memory with the increase in the size of the text files in the encoding and decoding processes, and the memory consumed in the decoding process was greater than the encoding process.

References

[1] Hussain, S., Jamal, S. S., Shah, T., & Hussain, I. (2020). A power associative loop structure for the construction of non-linear components of block cipher. IEEE Access, 8, 123492–123506.

[2] Shetty, V. S., Anusha, R., MJ, D. K., & Hegde, P. (2020). A survey on performance analysis of block cipher algorithms. 2020 International Conference on Inventive Computation Technologies (ICICT), 167–174.

[3] Ali, K. M., & Khan, M. (2019). A new construction of confusion component of block ciphers. Multimedia Tools and Applications, 78, 32585–32604.

[4] Al-Shammary, M. E. K., & Al-Dabbagh, S. S. M. (2022). Differential Distribution Table implementation DDT survey.

[5] Hendi, A. Y., Dwairi, M. O., Al-Qadi, Z. A., & Soliman, M. S. (2019). A novel simple and highly secure method for data encryption-decryption. International Journal of Communication Networks and Information Security, 11(1), 232–238.

[6] Smart, N. P. (2003). Cryptography: an introduction (Vol. 3). McGraw-Hill New York.

[7] Shareef, A. M., & Hasani, N. F. (2023). Develop a method for cryptography by using matrix transpose in linear algebra. AIP Conference Proceedings, 2414(1), 40035.

[8] Thakkar, B., & Thankachan, B. (2021). A multilevel approach of transposition ciphers for data security over cloud. GIS Sci. J, 8(5), 1732–1738.

[9] Shruthy, V. N., & Veerasamy, M. (2021). A hybrid combination of substitution and transposition ciphers for efficient encryption using graph labeling.

[10] Bitar, A. A., & Sujatha, V. (2021). Merging Vernam Cipher stream and Rail Fence Algorithms and How Effective They are on IoT Devices.

[11] Touil, H., EL AKKAD, N., & SATORI, K. (2020). Text encryption: hybrid cryptographic method using Vigenere and Hill Ciphers. 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), 1–6.

[12] Nahar, K., & Chakraborty, P. (2020). Improved approach of rail fence for enhancing security. International Journal of Innovative Technology and Exploring Engineering, 9(9), 583–585.

[13] Sehrawat, D., & Gill, N. S. (2018). Lightweight block ciphers for IoT based applications: a review. International Journal of Applied Engineering Research, 13(5), 2258–2270.

[14] Abdalrdha, Z. K., Al-Qinani, I. H., & Abbas, F. N. (2019). Subject review: key generation in different cryptography algorithm. Int J Sci Res Sci Eng Technol, 6(5), 230–240.

[15] Manucom, E. M. M., Gerardo, B. D., & Medina, R. P. (2019). Analysis of key randomness in improved one-time pad cryptography. 2019 IEEE 13th International Conference on Anti-Counterfeiting, Security, and Identification (ASID), 11–16.

[16] Ballard, L., Kamara, S., & Reiter, M. K. (2008). The Practical Subtleties of Biometric Key Generation. USENIX Security Symposium, 61–74.

[17] Bano, A. (2013). Random key generator using human voice. IMPACT-2013, 41–45.

[18] Kwok, H. S., & Tang, W. K. S. (2007). A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons & Fractals, 32(4), 1518–1529.

[19] Akhshani, A., Akhavan, A., Mobaraki, A., Lim, S.-C., & Hassan, Z. (2014). Pseudo random number generator based on quantum chaotic map. Communications in Nonlinear Science and Numerical Simulation, 19(1), 101–111.

[20] Kumar, A., & Dua, M. (2021). Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. Multimedia Tools and Applications, 80(18), 27785–27805.

[21] Kuznetsov, N., Mokaev, T., Ponomarenko, V., Seleznev, E., Stankevich, N., & Chua, L. (2023). Hidden attractors in Chua circuit: mathematical theory meets physical experiments. Nonlinear Dynamics, 111(6), 5859–5887.

[22] He, J., & El-Dib, Y. O. (2021). The reducing rank method to solve third-order Duffing equation with the homotopy perturbation. Numerical Methods for Partial Differential

Equations, 37(2), 1800–1808.

23 Wang, S., He, S., Yousefpour, A., Jahanshahi, H., Repnik, R., & Perc, M. (2020). Chaos and complexity in a fractional-order financial system with time delays. Chaos, Solitons & Fractals, 131, 109521.

[24] Bucolo, M., Buscarino, A., Fortuna, L., & Gagliano, S. (2022). Multidimensional discrete chaotic maps. Frontiers in Physics, 199.

[25] Souza, C. E. C., Chaves, D. P. B., & Pimentel, C. (2020). One-Dimensional Pseudo-Chaotic Sequences Based on the Discrete Arnold's Cat Map Over $\mathbb{Z}_3$m. IEEE Transactions on Circuits and Systems II: Express Briefs, 68(1), 491–495.

[26] Boullé, N., Dallas, V., Nakatsukasa, Y., & Samaddar, D. (2020). Classification of chaotic time series with deep learning. Physica D: Nonlinear Phenomena, 403, 132261.

[27] Ayubi, P., Jafari Barani, M., Yousefi Valandar, M., Yosefnezhad Irani, B., & Sedagheh Maskan Sadigh, R. (2021). A new chaotic complex map for robust video watermarking. Artificial Intelligence Review, 54, 1237–1280.

[28] Hua, Z., & Zhou, Y. (2019). Exponential chaotic model for generating robust chaos. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(6), 3713–3724.

[29] Naskar, P. K., Bhattacharyya, S., Nandy, D., & Chaudhuri, A. (2020). A robust image encryption scheme using chaotic tent map and cellular automata. Nonlinear Dynamics, 100, 2877–2898.

[30] Elghandour, A., Salah, A., & Karawia, A. (2022). A new cryptographic algorithm via a two-dimensional chaotic map. Ain Shams Engineering Journal, 13(1), 101489.

[31] Abdullah H. (2016). Performance Enhancement of Blowfish Algorithm in Data Encryption [Master Thesis]. Faculty of Electrical and Electronic Engineering, University of Aleppo.