Binary columnar transposition cipher

Fouad Sahib Muhamed Alkhazraji[1]
fouadalkhazraji8@gmail.com

Abstract: Cryptography is the way to keep our information safe from intruders. Transposition is a cipher technique that has been used historically to encrypt and decrypt messages. Stream and block cipher is a modern technique that has been used to deal with binary numbers. This paper uses the Columnar Transposition Cipher (CTC) method which is a type of transposition technique to enhance using the Block cipher technique. Using this combination of ciphers, makes the algorithm more complicated and secure. It makes it difficult for attackers to analyze the results and break the cipher.

Keywords: Cryptography, CTC, BCTC, Stream, Block, Transposition

1. Introduction

Encryption is the way to transform a text or any file from readable form (plain text) into unreadable form (Ciphertext). It is the way to save our information from attackers. Decryption is the way to transform the text or any file from unreadable form into readable form [1]. Because of using stream or block cipher which is a bit-oriented method, combining Classical and Modern ciphers is more secure than combining Transposition and Substitution ciphers which is the character-oriented method [2].

2. Cryptography

It is classified into Symmetric Cryptography (SC) and Asymmetric Cryptography (AC). The first one uses the same key for both encryption and decryption. It is easy to perform, but the main disadvantage is that the attacker can discover the whole information in case of knowing the key. In AC there is two different keys are used, a public one for encryption and a private one for decryption. The public one is known for all senders and the private one is known only for the receiver. The main disadvantage is that AC is slower than SC [3].

[1] Assist. Lecturer: Administrative and Financial Directorate, Ministry of Higher Education and Scientific Research, Iraq.

2.1 Cryptography Dimensions

- Encryption Technique which includes substitution and transposition.
- Key numbers include single key and double key.
- Processing way which includes stream and block.

2.2 Cryptography Services

Confidentiality: only authorized parties can access transmitted information.
Authentication: received information should arrive from an authorized source identity.
Integrity: information being transmitted should be modified by authorized people only.
Access control: only authorized people access the resources and control what they are allowed to do.
Non-Repudiation: enforce entities not to deny the participation in part or all communication which have been involved in.

3. Substitution and Transposition Techniques

Encryption techniques are two basic building blocks: Substitution and Transposition. With Substitution, there is a replacement between letters, numbers, or symbols to produce Cipher text from Plaintext. In the case of binary representation, the replacement is performed with bit patterns. Examples of substitution techniques are Caesar Cipher, Hill Cipher, Playfair Cipher, Monoalphabetic, Cipher, and Polyalphabetic Cipher. with Transposition there is a permutation and rearrangement for Plaintext letters. Examples of Transposition techniques are the Rail Fence technique, Odd-Even, and Column Transposition.

4. Classical and modern cryptography

Here the classification depends on the periods when the cryptography algorithm was used or developed. The Classical ones were developed first in history and still some of them are used in the present time as they provide information confidentiality. The Modern ones were developed recently and they are complex more than the Classical ones [4].

5. Stream cipher (SC) and Block Cipher (BC)

They are a bitwise coding which algorithm of cryptography performed on each binary digit. In SC one bit of keystream is generated each time. This bit is used in the process of both encryption and decryption [5]. There are two types of SC, synchronous and asynchronous. The synchronous one is when depending only on the key to produce keystream. The asynchronous one is when depending on the

key and the Ciphertext to produce keystream. The security assessment is not easy to be precise when using SC in encryption. With block cipher, the bit-string is divided into blocks with specific sizes. There are many applications used with block ciphers that can provide data integrity, confidentiality, and user authentication. Sometimes, stream ciphers used block ciphers as key stream generators [2].

6. Rail Fence Cipher (RFC)

It is one type of Transposition Ciphers. Its mechanism is to write the Plaint text letter by letter on alternate lines diagonally. The next step is to append all lines in one independent line. The key is the number of lines to use, which is called the depth of the Rail Fence.

7. Columnar Transposition Cipher (CTC)

It is another type of Transposition Ciphers that rearranges the characters or bits of the plaintext into columns. The key is the order of the columns. For example, imagine the key is 3412 and the plaintext is "SECURITY IS THE FUN ". The cipher will be as below:

3	4	1	2
S	E	C	U
R	I	T	Y
I	S	T	H
E	F	U	N

After reading the letters column by column the Ciphertext will be "CTTUUYHNSRIEEISF" [6].

8. Related work

In [5] the authors designed a method called LIZARD IP core. For encryption, keystream XORed with Plaintext to generate Ciphertext. For decryption, Ciphertext XORed with the keystream to generate the Plaintext. The method takes six inputs: 120-bit key, 64-bit Initialization Vector (IV), 119 -bit Plaintext, Reset, Clock, and Enable. The process of state initialization has four phases to generate the keystream: Key and IV loading, Grain like Mixing, 2nD key addition, and Final Diffusion. They claimed that their method is so efficient against Time Memory Data Tradeoff (TMTD) and key recovery attacks. They made stream cipher more complicated to be broken by attackers.

In [7] The authors modified a new method by mixing steps of Caesar Cipher with Vigenere Cipher. The process of their method is by choosing a numbered key and a lettered key. Performing Caesar Cipher on lettered key using the shift of numbered key to produce a new key. Using the new key to perform Vigenere Cipher on the Plaintext. Using the binary representation of the numbered key to XOR it with the first generated letter of the Ciphertext. The result is XORed with the next letter of the Ciphertext generated and the process continues till covering the complete generated Ciphertext. The Ciphertext in binary form is converted into ASCII Table and finally gets the form of alphabet, numbers and symbols as a final Ciphertext. They claimed that the new version is hybrid and is very hard to be break by frequency method and brute force.

9. The Proposed Algorithm (Binary CTC)

In our proposed algorithm we are going to change any type of file into binary type, so we can deal with it in a binary way. Saving the binary contents of the file in an array and it should have enough size to contain all the bits. It considers the entire array of the bits as one block. The method needs to select a suitable key to perform CTC on the array. It uses CTC to manipulate the Plaintext block. Because we change the file directly into binary form, we got a transmitted array of bits that has no spaces, so it doesn't need to deal with them. The method uses the same key for encryption and decryption.

9.1 Steps of the encryption

Step1: Change the plaintext file from its original format into binary format and save it in an array.
Step2: select the key.
Step3: perform the CTC encryption process on the array by using the selecting key to obtain a new array.
Step4: Change the new array from binary format into the original format to obtain a Ciphertext file.

9.2 Steps of the decryption

Step1: Change the Cipher text file from its original format into binary format and save it in an array.
Step2: select the same key.
Step3: perform the CTC decryption process on the array by using the selecting key to obtain a new array.
Step4: Change the new array from the binary format into the file original format to obtain the plain text file.

Figure 1 explains the mechanism of BCTC for Encryption and Decryption.

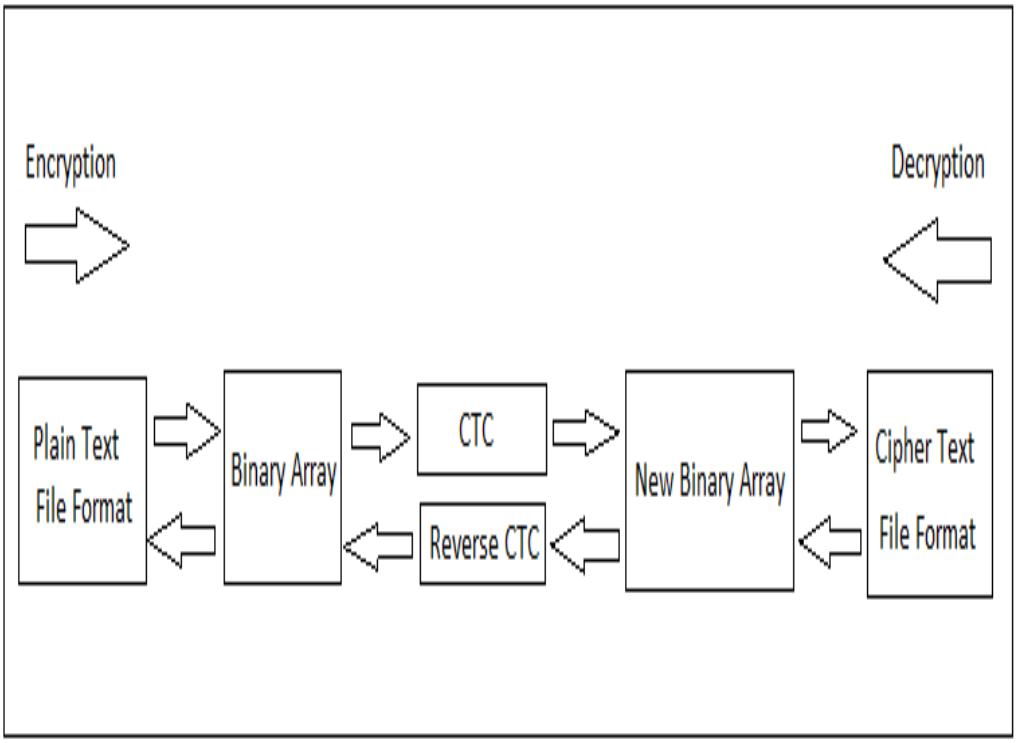

Figure 1: BCTC Mechanism: Encryption & Decryption

10. Results and Discussion

Imagine, for example, changing the Plaintext file from its format into binary format and saving it in a single array. Probably we will get an array with a big size but in this example, we will use an array with a small size just for explanation.
Encryption: This is a binary array with a size of 19 numbers:

0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Firstly, performing CTC on it and distributing it into a matrix with the key of 3412:

3	4	1	2
0	1	0	1
0	1	0	1
0	1	0	1
0	1	0	1
0	1	0	

The last position at the end of the matrix is empty. Therefore, the program doesn't reach it and ignores it by the formula that has been used in the code. Secondly, we are going to arrange it again column by column starting by the third one and ending by the second one according to the key we have which is 3412 to obtain this array:

0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	1	1	1

Finally, we converting the array from binary format into its original file format to obtain the final Ciphertext file.

Decryption: Firstly, converting the final Ciphertext file from its original format into binary format to get this array:

0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	1	1	1

Secondly, performing CTC on the array and distributing its numbers into the matrix vertically with the same key of 3412:

3	4	1	2
0	1	0	1
0	1	0	1
0	1	0	1
0	1	0	1
0	1	0	

Finally, reading each line horizontally and save it in the array:

0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Generally, in performing CTC, there is a problem of dealing with the extra values that exist at the end of the matrix. To solve the problem, the program handles all the possibilities that occur through performing CTC processes. Because the key length is no more than ten digits from 0-9, there are nine different possibilities that happen in the last row as a maximum range. Figure 2 explains the possibilities of the CTC extra values:

0	0	0	1	0	0	0	0	0	0
1	1	0	1	0	1	0	1	0	0
0	0	0	0	0	0	0	0	0	1
0	0	0	1	0	0	1	1	0	0
0	0	0	1	1	1	0	0	0	1
0	0	0	1	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	0
0	x	x	x	x	x	x	x	x	x

Figure 2: Matrix Shows the Extra Values

To find the number of the values of the last row of the matrix, we use this equation:

$$ValusLastRow = TextLength \bmod keyLength \quad (1)$$

To find the number of the values of Xs that we add to the last row of the matrix, we use this equation:

$$XNum = keyLength - (TextLength \bmod keyLength) \quad (2)$$

Practical example results:
After performing our java program method to **encrypt** a text composed of 83 bits and the key (1567082493), we got the results as below:

Enter Plain Text:
11111111110000000000101010101010101010101010101000000000000111111
11110101010101010

PlainText Length : 83 Bits
Key Length : 10 Rooms
Num of Rows : 9 Rows
Values Last Row : 3 Values

CTC Encryption Matrix:
1111111111
0000000000
1010101010
1010101010
1010101010
0000000000
1111111111
0101010101
010

Cipher Text Length: 83 Bits
10111010101110100101110101000001110000011100000111101110100100000 1
11000001110111010

After performing our java program method to **decrypt** the Ciphertext composed of 83 bits and the key (1567082493), we got the results as below:

Cipher Text Length : 83 Bits
Key Length : 10 Rooms
Num of Rows : 9 Rows
Values Last Row : 3 Values

CTC Decryption Matrix:

1111111111
0000000000
1010101010
1010101010
1010101010
0000000000
1111111111
0101010101
010

Plain Text Length: 83 Bits
11111111110000000000101010101010101010101010101000000000000111111
11110101010101010

11. Conclusions

The proposed method enhances the security of both block and columnar cipher. It makes it more complex and hard to be broken by attackers. The paper went through mixing classical and modern ciphers to obtain a hybrid cipher. It explains the features of Cryptography Dimensions and Services in addition to Substitution and Transposition Techniques. Java program has been used to perform CTC in encryption and decryption on a binary array.

12. References

[1] Agrawa, A., Amet, G. K., & Arya, A. D. (2019). Secured Symmetric Key Encryption Algorithm with Modified Rail Fence Technique. International Journal of Research and Scientific Innovation (IJRSI), 6(4), 93-99 URL: https://www.rsisinternational.org/journals/ijrsi/digital-library/volume-6-issue-4/100-106.pdf.

[2] ABDEL Wahab O. F, Khalaf A. A. M., Hussein A. I. & Hamed H. F. A.. (2021). Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. in IEEE Access, 9, 31805-31815. URL: https://ieeexplore.ieee.org/document/9356603

[3] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein and H. F. A. Hamed, (2021) 'Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques', in

IEEE Access, vol. 9, pp. 31805-31815. Available at: https://ieeexplore.ieee.org/document/9356603

[4] Poonia,P. & Kantha, P. (2016). Comparative Study of Various Substitution and Transposition Encryption Techniques. International Journal of Computer Applications, 145 (10), 0975 – 8887. URL: https://www.ijcaonline.org/archives/volume145/number10/25315-2016910783

[5] Nandakumar, R., Thomas, T., & Jose ,J. K. (2019). Design and Characteristics of LIZARD Stream Cipher IP Core. International Research Journal of Engineering and Technology(IRJET), 6(6) 3036-2040. URL: https://www.irjet.net/archives/V6/i6/IRJET-V6I6617.pdf

[6] Saranya, R., & Kingslin, S. (2018). Evaluative Study on Substitution and Transposition Ciphers. International Journal of Creative Research Thoughts (IJCRT),6(1) 155-160. URL: http://www.ijcrt.org/papers/IJCRT1801021.pdf

[7] Omolara1, O.E., Oludare, A.I. & Abdulahi, S.E.(2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication. Computer Engineering and Intelligent Systems, 5 (5) 34-46. URL: https://core.ac.uk/download/pdf/234644813.pdf

تشفير التحويل العمودي للأرقام الثنائية

فؤاد صاحب محمد الخزرجي[1]
fouadalkhazraji8@gmail.com

المستخلص: التشفير هو وسيلة للحفاظ على معلوماتنا بصورة آمنة من المتسللين. التحويل هو أسلوب تشفير تم استخدامه تاريخيًا لتشفير وفك تشفير الرسائل. التشفير الآني والكتلي هو أسلوب حديث يستخدم للتعامل مع الأرقام الثنائية. يستخدم هذا البحث طريقة التشفير العمودي (CTC) وهو نوع من تقنيات التحويل لتحسين استخدام تقنية التشفير الكتلي. باستخدام هذا المزيج من التشفير تكون الخوارزمية أكثر تعقيدًا وأمانًا بحيث يصعب على المهاجمين تحليل النتائج وكسر الشفرة.

الكلمات المفتاحية: التشفير ، CTC، BCTC ، تشفير آني ، تشفير كتلي ، تحويل .

[1] مدرس مساعد: الدائرة الادارية و المالية - وزارة التعليم العالي و البحث العلمي - بغداد - العراق