Modifying Playfair Cipher Algorithm by using Legendre Symbol

Hamza B. Habib

Department of Mathematics – College of Science – University of Diyala

halsaadi18@yahoo.com

Received: 24 April 2019 **Accepted: 23 May 2019**

DOI: https://dx.doi.org/10.24237/djps.15.04.502A

Abstract

In recent years, transmitting data on the Internet became a daily usage of people, such as sending emails, online shopping and so on. Generally, this data should be confidential and hence it should be secured by using cryptosystem algorithms. A new algorithm of securing the transmitted data by combining Playfair Cipher with Legendre symbol is presented in this paper. In this algorithm a large prime number P can be chosen by both of sender and the receiver in order to calculate Legendre Symbol $\left(\frac{a}{P}\right), \forall\ 1 \leq a \leq P-1$ and then sorting them in a random order set. Moreover, as Legendre symbol is either 1 or -1, then this helps them in the proposed algorithm to use two tables with two keywords for the encryption and decryption processes instead of using only one table and one keyword as in the standard Playfair cipher algorithm. Thus, our proposed algorithm increases the security level of the transmitted data on the insecure channels comparing with the standard algorithm.

Keywords: Playfair cipher, Cryptosystem, Number Theory, Legendre Symbol.

Diyala Journal for Pure Science

Modifying Playfair Cipher Algorithm by using Legendre Symbol

Hamza B. Habib

تعديل خوارزمية شفرة بليفير بأستخدام رمز ليجيندرا

حمزة بركات حبيب

قسم الرياضيات – كلية العلوم – جامعة ديالى

الخلاصة

في السنوات الأخيرة، أصبح نقل البيانات على الإنترنت استخدامًا يوميًا للأشخاص، مثل إرسال رسائل البريد الإلكتروني والتسوق عبر الإنترنت وما إلى ذلك. بشكل عام، هذه البيانات يجب أن تكون سرية وبالتالي يجب تأمينها باستخدام خوارزميات التشفير. خوارزمية جديدة لتأمين البيانات المنقولة قد تم تقديمها في هذا البحث من الجمع بين خوارزمية شفرة بليفير مع رمز ليجيندرا. في هذه الخوارزمية يتم اختيار عدد اولي كبير من قبل كل من المرسل والمستلم لحساب رمز ليجيندرا $\left(\frac{a}{P}\right)$ لكل $1 \leq a \leq P-1$ ومن ثم ترتيبها عشوائيا في مجموعة. بالأضافة , بما أن رمز ليجيندرا هو أما 1 أو -1 فأن هذا يساعدهم في الخوارزمية المقترحة بأستخدام جدولين مع كلمتين دالتين أثنتين لعمليات التشفير وفك التشفير بدلا من استخدام فقط جدول واحد وكلمة دالة واحدة كما هو موجود في خوارزمية التشفير بليفير الأعتيادية. ولذلك، الخوارزمية المقترحة تزيد من مستوى أمان البيانات المرسلة عبر القنوات غير الآمنة مقارنة بالخوارزمية الأعتيادية.

الكلمات المفتاحية: شفرة بليفير، التشفير، نظرية الأعداد، رمز ليجيندرا.

Introduction

Securing the transmitted data mathematically over the unsecure channels can be achieved by using cryptosystem algorithms [1]. One of those algorithms is Playfair cipher which uses a 5×5 table of 25 unduplicated English alphabets with a keyword is inserted in the table. This algorithm can be hacked easily by the existence of computers, see [2].

Several researches have been done to modify Playfair cipher in the last few years. For example, Bhattacharyya et al. [1] argue that the standard Playfair cipher, which uses 5×5 table and a keyword is placed in that table, can be safer by using six 10×9 tables with six iterations. Six iterations based on encoding the message six times by using in turn six distinct 10×9 tables, such that, each table contains a keyword. This method also can be used for the decryption. Murali and Senthil Kumar [2] claim that the security of transmitting data over unsecured classical channels is increased by combining Playfair cipher with Linear Feedback Shift Register (LFSR). LFSR is used to generate random numbers in order to transmit them instead of the corresponding letters.

Iqbal et al. [3] present an algorithm of Playfair cipher by using Excess 3 Code (X S3) with Ceasar Cipher. This algorithm uses a 6×6 table containing only integers and alphabets. However, those integers and alphabets should be converted into binary numbers first then to their excess 3 code before transmitting them.

Khan [4] provides a comparison of matrices of distinct sizes, which are 9×9, 10×10 and 11×11. The comparison results say that the efficiency of the encryption increases with increasing the size of the matrix. However, the size of the plaintext will not have an interesting impact on the outcome of the encryption. While, increasing the size of the keyword leads to increase the encryption efficiency.

Eweoya et al. [5] propose an improved version of Playfair cipher by using a 16×16 table of ASCII codes. Using the ASCII codes makes this version neglects the restriction in the standard Playfair cipher of using only 26 letters because ASCII codes allows it to use any other characters. Also, by using the Advanced Encryption Standard makes this version stronger.
Kansal et al. [6] also state that, Playfair cipher can be modified by using the properties of each of ``DNA strands" and amino acids. This modification is based on converting the plaintext (before the encryption has been done) in turn to the forms: binary, DNA, and finally to the amino acid form. Thus, the plaintext can be extended to have alphabetical form (upper or lower cases) and numerical form without omitting the punctuations.

Tunga and Mukherjee [7] argue that Playfair cipher can be improved by using Frequency Analysis. Firstly, using this method helps to remove some of Playfair cipher weakness. For example, identifying whether the letter X in the plaintext has been added to it or it is an actual letter of it and the existence of the spaces in the plaintext. Secondly, providing a method of supplying keywords can increase the safety of the transmitted information. Finally, extending the size of the table to 16×16 and modifying it makes the plaintext includes a large range of ASCII codes. However, the improved version of Playfair cipher has some disadvantages, such as, it can be hacked easily if the algorithm is known for the hacker because the information is sorted in the tables. Also, there are many characters in the table will not be used in the algorithm.

In this paper, we present a proposed algorithm that is based on using Legendre symbol with Playfair cipher. Using Legendre symbol helps us to use two tables with two secret keywords instead of only one table and one keyword in order to increase the security of the transmitted data.

The rest of the paper is structured as: we explain the standard Playfair cipher algorithm in the next section. We follow that by giving the basic notions regarding Legendre Symbol. Then, we introduce the proposed algorithm of modifying the Playfair cipher by using Legendre symbol. Also, we provide a working example of the proposed algorithm. Finally, in the last section the conclusion is provided.

The Standard Playfair Cipher Algorithm

Playfair algorithm firstly introduced in 1854 by Charles Wheatstone; however, it was named after Lord Playfair for promoting the use of it [4].

The standard Playfair cipher algorithm is based on using a 5×5 table of unduplicated English letters. A unique keyword, which is chosen by both the sender and receiver, is placed in the table starting from the left top. The rest of spaces in the table are filled by the rest of alphabets; however, there are 26 letters, then usually J is either omitted or placed in the same place of I in the table, see [8].

To do the encryption process, then the sender breaks the plaintext (omitting the spaces and the punctuations) into pairs of letters and follows the simple rules below, see [9]. If the number of letters in the plaintext is an odd number then a letter X is placed in the end. Also, if there is a pair of letters contains duplicated letters, then X is placed in between them to separate them.

1. If the pair of letters appears in the same row, then each letter is replaced by the letter to the right of it (consider the wrapping around if we reached the end of the table).
2. If the pair of letters appears in the same column, then each letter is replaced by the letter beneath it (consider the wrapping up if he reached the end of the table).
3. If the pair of letters does not satisfy the rules 2 and 3, then each letter of them on a formed rectangle corner is replaced with the one on the opposite corner (without omitting the order).

The decryption process is done by the receiver by reversing the last three rules, 2, 3 and 4 and by omitting all of the extra X's, if there were any, to get the original message, [9].

Legendre Symbol

In this section we give simple notions to explain Legendre symbol. Suppose that k is an integer and n is a positive integer, if $k \not\equiv 0\ (mod\ n)$ and the quadratic congruence $x^2 \equiv k\ (mod\ n)$ has a solution, then a is called a quadratic residue modulo n. Otherwise k is called a quadratic nonresidue modulo n, see [10]. The most important case in the quadratic congruences is when n is prime and $k\ \not\equiv 0\ (mod\ n)$. Therefore, in this paper we are interested in this case, and noting that P referrers to the prime number.

Legendre symbol $\left(\frac{k}{P}\right)$ can be considered as an interesting subject in Number Theory; it can be defined as, if P is an odd prime and k is an integer with $k\ \not\equiv 0\ (mod\ P)$, then [10]:

$$\left(\frac{k}{P}\right) = \begin{cases} 1, & \text{if } k \text{ is a quadratic residue;} \\ -1, & \text{if } k \text{ is a quadratic nonresidue.} \end{cases}$$

Theorem 1

(Euler's Criterion) [8] If P be an odd prime, k is a positive integer and $k\ \not\equiv 0\ (mod\ P)$, then

$$\left(\frac{k}{P}\right) \equiv k^{\frac{(p-1)}{2}}\ \ (mod\ P).$$

Theorem 2

(Properties of Legendre Symbol) If P is an odd prime and both of k and l are positive integers, such that, $k, l \not\equiv 0 \ (mod\ P)$, see [10], [11] then

a) If $k \equiv l \ (mod\ P) \Longrightarrow \left(\frac{k}{P}\right) \left(\frac{l}{P}\right)$,

b) $\left(\frac{k}{P}\right)\left(\frac{l}{P}\right) = \left(\frac{kl}{P}\right)$,

c) $\left(\frac{k^2}{P}\right) = 1$.

Legendre Symbol can be related to the Quadratic Reciprocity Law in an interesting way as shown in the theorem below.

Theorem 3

If P and Q are two odd distinct primes, then [12], [13]

1) $\left(\frac{-1}{P}\right) = -1^{\frac{(p-1)}{2}} = \begin{cases} 1, & if\ P \equiv 1 \ (mod\ 4); \\ -1, & if\ P \equiv 3 \ (mod\ 4). \end{cases}$

2) $\left(\frac{2}{P}\right) = (-1)^{\frac{(P^2-1)}{8}} = \begin{cases} 1, & if\ P \equiv 1 \text{ or } 7 \ (mod\ 8); \\ -1, & if\ P \equiv 3 \text{ or } 5 \ (mod\ 8). \end{cases}$

3) Quadratic Reciprocity Law: $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{(P-1)(Q-1)}{4}}$.

Proposed Algorithm

The proposed algorithm is based on using Legendre Symbol $\left(\frac{a}{P}\right)$, and that leads to use two tables, Table 1 and Table 2. Then the sender and receiver select:

1. Keyword 1 for table 1.

2. Keyword 2 for table 2.

3. A large prime number P, then calculating Legendre Symbol $\left(\frac{a}{P}\right)$, for all a, where $1 \leq a \leq P-1$ by using the suitable formulas that are given before. Then, they sort Legendre symbol in a set in an agreed randomly order to increase the difficulty level of the algorithm.

As we discussed in a previous section, using the same way of inserting the keyword in the table, the keywords 1 and 2 can be inserted by both the sender and receiver in the tables 1 and 2 respectively.

Moreover, based on the value of Legendre symbol, the formula 1 below, which is known for both the sender and receiver, identifies which table can be used to encrypt and decrypt the messages.

$$\left(\frac{a}{P}\right) = \begin{cases} \mathbf{1}, & \boldsymbol{use\ table\ 1}; \\ \mathbf{-1}, & \boldsymbol{use\ table\ 2}. \end{cases} \qquad \textbf{(1)}$$

Also, by following the same rules of encryption and decryption processes that given in Section II, the data can be transmitted safely.

Applied Example

Suppose that both of the sender and the receiver agreed on

Keyword 1 is GEOMETRY.

Keyword 2 is SQUARES.

For simplicity, let P = 23, and let Legendre symbol is calculated and sorted randomly in the set {6, 14, 2, 8, 5, 20, 3, 7, 10, 15, …}. Then, the tables are:

Table 1: Keyword 1 is inserted here

G	E	O	M	T
R	Y	A	B	C
D	F	H	I / J	K
L	N	P	Q	S
U	V	W	X	Z

Table 2: keyword 2 is inserted here

S	Q	U	A	R
E	B	C	D	F
G	H	I / J	K	L
M	N	O	P	T
V	W	X	Y	Z

Encryption Process

Suppose the plaintext message is "COMMUNITY", then it should be broken into: "CO MM UN IT Y" which can be written as "CO MX MU NI TY" after placing the letter X in between the repeated letters MM to separate them. The sender needs to calculate Legendre Symbol as below, and using formula 1 in the previous Section, then

$\left(\frac{6}{23}\right) = 1 \Longrightarrow$ using table 1 we get CO $\longrightarrow$ AT,

$\left(\frac{14}{23}\right) = -1 \Longrightarrow$ using table 2 we get MX $\longrightarrow$ OV,

$\left(\frac{2}{23}\right) = 1 \Longrightarrow$ using table 1 we get MU $\longrightarrow$ GX,

$\left(\frac{8}{23}\right) = 1 \Longrightarrow$ using table 1 we get NI $\longrightarrow$ QF,

$\left(\frac{5}{23}\right) = -1 \Longrightarrow$ using table 2 we get TY $\longrightarrow$ PZ.

Thus, the encoded message is "ATOVGXQFPZ" which will be sent to the receiver.

Decryption Process

After the encoded message "ATOVGXQFPZ" is received, the receiver breaks it into "AT OV GX QF PZ" and starts calculating Legendre symbol as below and using formula 1, then

$\left(\frac{6}{23}\right) = 1 \Longrightarrow$ using table 1 we get AT $\longrightarrow$ CO,

$\left(\frac{14}{23}\right) = -1 \Longrightarrow$ using table 2 we get OV $\longrightarrow$ MX,

$\left(\frac{2}{23}\right) = 1 \Longrightarrow$ using table 1 we get GX ⟶ MU,

$\left(\frac{8}{23}\right) = 1 \Longrightarrow$ using table 1 we get QF ⟶ NI,

$\left(\frac{5}{23}\right) = -1 \Longrightarrow$ using table 2 we get PZ ⟶ TY.

Thus, the original plaintext is "COMMUNITY" after omitting the letter X.

Experimental Results

In this study, Legendre Symbol adds the feature to the encryption and decryption processes in Playfair algorithm of utilizing two agreed tables and keywords. Also, an agreed odd prime is chosen in order to generate a random Legendre Symbols list. As the list is randomly ordered, then using table 1 and table 2 is based on the resulting value of Legendre symbol in this list.

To analyze Playfair Cipher then we need to discuss the permutation of the table that consists of the 25 letter cipher alphabets. The total number of this permutation is

$$25! = 1 \times 2 \times \cdots \times 25 = 1551121 \cdots.$$

By continually moving the columns and/or rows around, we can choose any of the 25 letters and move it to any wanted position in the table. As a result of that then the positions of the remaining letters will be fixed, that is, each table fits in a class of 25 equivalent tables. Then the total number of these equivalence classes is

$$\frac{25!}{25} = 24! = 1 \times 2 \times \cdots \times 24 = 6204484 \cdots$$

Which is,

$$24! \approx 2^{79}.$$

That means, the number of equivalence classes of Playfair tables approximately matches the number of 79-bit bit strings, which equals to say the 80-bit keys of the modern cipher (Block Cipher). Block Cipher would require massive and expensive computing processes.

Thus, from the results that we have obtained we can deduce that the probability attack on the ciphertext to find the original plaintext in the standard Playfair Cipher is 1/676, while it is 1/456976 in the case of using the proposed Playfair algorithm.

Therefore, from above we can say that the proposed algorithm is much safer and complicated for the attackers.

Conclusion

In this paper, we have presented a modified and secure version of Playfair cipher by using Legendre symbol. Employing Legendre Symbol, which is based on using large prime and a random sorting order set of Legendre, in the algorithm provides the fact of using two keywords and two tables instead of only one keyword and one table. Also, as there are 26 alphabetical letters, then in the standard Playfair algorithm there are only 26 x 26 = 676 pair of letters. While, the proposed algorithm provides the use of two tables, that means there are 676 x 676 = 456976 pair of letters. Thus, the modified algorithm increases the protection of the transferred data on the Internet and hence this makes the hacking modified algorithm is difficult to be done. For future research, the proposed algorithm can be applied for extended table sizes.

Reference

1. S. Bhattacharyya, N. Chand, S. Chakraborty, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 3(2), pp. 307-312 (2014).
2. P. Murali, G. Senthilkumar, IJCSNS International Journal of Computer Science and Network Security, 8(12), pp. 26-29 (2008).
3. Z. Iqbal, B. Gupta, K. Kr. Gola, P. Gupta, International Journal of Computer Applications, 103(13), pp. 16-20 (2014).

4. S. A. Khan, International Journal of Computing and Network Technology, 3(3), pp. 117-122 (2015).

5. I. Eweoya, O. Daramola, N. Omoregbe, Covenant Journal of Informatics and Communication Technology (CJICT), 1(2), pp. 79-88 (2013).

6. A. Kansal, S. Sneha, M. K. Patel, International Journal of Education and Science Research Review, 3(2), pp. 1-9 (2016).

7. H. Tunga, S. Mukherjee, International Journal of Emerging Technology and Advanced Engineering, 2(1), pp. 100-290 (2012).

8. A. A. Alam, B. S. Khalid, C. M. Salam, International Journal of Computer Theory and Engineering, 5(4), pp. 626-628 (2013).

9. R. Deepthi, International Research Journal of Engineering and Technology (IRJET), 04(04), pp. 2607-2610 (2017).

10. K. H. Rosen, Elementary number theory and its applications, 6th ed (Addison-Wesley, Pearson, 2011), pp. 288- 335.

11. B. Karaivanov, T. S. Vassilev, Integers, 16(2), pp. 1-10 (2016).

12. D. Alkema, The Law of Quadratic Reciprocity from Fermat to Gauss, Thesis, University of Utrecht, Netherlands, (2016).

13. Gauss, C. F., and A. A. Clarke. "Disquisitiones Arithmeticae, Leipzig." Translated into English by Arthur A. (1966), Quotations are from the English translation. Google Scholar (1801).