Modified Block Playfair Cipher using Random Shift Key Generation

Arvind Kumar
Galgotias College of Engineering and Technology, Greater Noida

Pawan Singh Mehra
Galgotias College of Engineering and Technology, Greater Noida

Gagan Gupta
Galgotias College of Engineering and Technology, Greater Noida

Aatif Jamshed
Galgotias College of Engineering and Technology, Greater Noida

ABSTRACT

In this paper conventional Playfair Cipher is being modified by encrypting the plaintext in blocks. For each block the keyword would be the same but the matrix will shift by some random value. As a result of which the diagram analysis would be very difficult which is done in the traditional Playfair Cipher to obtain the plaintext from the ciphertext. The shift value will be generated using SHA-1 which is very secure. Playfair Cipher method, based on polyalphabetic cipher is relatively easy to break because it still leaves much of the structure and a few hundred of letters of ciphertext are sufficient. To add to its security and to make it more usable we are using 6x6 matrix instead of 5x5 which will be able to cover 26 alphabets in English and ten numerals i.e. from 0 to 9. This 6x6 matrix eliminate the case of putting of 2 alphabets (I and J) together in the matrix as it was in the 5x5 matrix. Plaintext as well as key can be numeral, alphabetic or combination of both.

Keywords- Playfair Cipher; Random number; SHA-1; Polyalphabetic cipher

1. INTRODUCTION

Monoalphabetic substitution ciphers are easy to break because they reflect the frequency data of the original alphabet. That is ,they easily reflect the statistical structure of the plaintext in the ciphertext, since a particular alphabet in the plaintext is always replaced by another alphabet in the ciphertext as in the case of Caeser Cipher. That is why they are prone to cryptanalysis where a cryptanalyst exploits the regularities of the language which is actually the letter frequency of the English alphabets .One principle method that is used in substitution ciphers to lessen the extent to which the structure of the plaintext survives in the ciphertext is to encrypt the multiple letters of the plaintext in ciphertext. The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams. The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. The Playfair cipher is a great advance over simple monoalphabetic ciphers. For one thing, whereas there are only 26 letters, there are 26x 26 = 676 digrams, so that identification of individual digrams is more difficult. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult. For these reasons, the Playfair Cipher was for a long time considered unbreakable. Despite this level of confidence in its security, the Playfair cipher is relatively easy to break because it still leaves much of the structure of the plaintext language intact. In this case we use digram frequencies of English letters. Other drawback of the traditional playfair cipher is that the letter I and J are considered as same in the plaintext, so overhead is created in distinguishing I and J during decryption. In modified version of the playfair cipher we have used 6x6 matrix that is capable of encrypting 26 alphabets and 10 digits(10 + 26=36).It has also addressed the problem of encrypting I and J as different alphabets as shown in matrix 1.

Matrix 1: 6x6 matrix of alphabets and digits

A	B	C	D	E	F
G	H	I	J	K	L
M	N	O	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Also what makes it more secure is that we are encrypting the plaintext in blocks. For each block the matrix is shifted by some random value, due to which the corresponding positions of the letters are changed, which adds to lot of confusion in the mind of cryptanalyst and makes it more secure towards attacks in which the attacker tries to exploit the statistical structure of the plaintext revealed in the ciphertext. This block version conceals the statistical structure to a great extend and makes it secure against cryptanalysis. To add to its security we are using SHA-1 for generating random numbers that will shift the matrix for each block.

There are many ways of generating random numbers but one of the most secure ways is to use SHA(Secure Hash Algorithm) for the purpose. Many languages like Java provides abstraction over the complexity of the algorithm. Java provides a class SecureRandom defind in java.Security that can be used to generate random numbers. SecureRandom uses the SHA-1 message digest algorithm, which produces a 20-byte digest. The SecureRandom is created using a seed. The seed value is digested, and the resulting value is stored as part of the SecureRandom's internal state. An internal counter is initialized to zero. Every time SecureRandom needs to create more pseudo-random numbers, the message digest is updated with the internal state and the counter, which is incremented. This data is digested and returned as the new pseudo-random data. The rest of the paper is organized as follows: Section II demonstrates the working of traditional Playfair Cipher and its related approaches. Section III

illustrates modified Block Playfair approach . Section IV is concerned with the analysis of the proposed algorithm and Section V summarizes the paper.

2. RELATED WORK

The Playfair Cipher shows a great improvement over the monoalphabetic ciphers. The identification of diagrams is more difficult than individual letters. In the monoalphabetic cipher, the attacker searches in 26 letters only. But by using the Playfair Cipher, the attacker has to search in 26 x 26 =676 digrams [1][2][3]. The relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult. The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. In this case, the keyword is *CRYPT*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order as shown in the matrix 2. The letters I and J count as one letter [4][8][9].

Matrix 2 : 5x5 matrix for traditional Playfair

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

Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that calling would be treated as ca lx li ng.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ab is encrypted as BD.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, hn is encrypted as NV.
4. Otherwise, each plaintext letter in a pair is the column occupied by the other plaintext letter. Thus, ao becomes DM and bq becomes EN.

In [3] the traditional Playfair Cipher has been combined with random number generator method. One of the simplest methods of random number generation called linear feedback shift register is used. Mapping is being done with random numbers to secret key of Playfair cipher method and corresponding numbers are transmitted to the recipient instead of alphabetical letter [5][6][7].

3. MODIFIED BLOCK PLAYFAIR APPROACH

In the conventional Playfair Cipher the same matrix is used to encrypt the entire plaintext, as a result of which it is vulnerable to cryptanalysis because it leaves the statistical traces of the plaintext in the ciphertext. In our modified version we are encrypting the plaintext in blocks .For each block the keyword would be the same but the matrix will shift by some value as shown in the figure. As a result of which the diagram analysis would be very difficult which is done in the traditional Playfair Cipher to obtain the plaintext from the ciphertext. The shift values will be random values, these random values can be generated through various ways, most common among them is linear feedback shift register but a more safe way of generating random numbers is through SHA-1 which takes a message digest of 20 bytes and generates random numbers. It is also hard to predict the random numbers if we have the previous one. Through this technique each time we will encrypt the same plaintext the output will be different. Suppose we have a plaintext which is divided into two blocks, so we need two random numbers. Each random number will be used to shift the matrix after the previous block has been encrypted, as a result of which the corresponding position of the letters to each other will be changed for the next block and the statistical traces will be concealed in the ciphertext. Also the block size can be chosen according to the requirement. If we want more security against cryptanalysis attacks , then the block size can be as small as 32 characters. In this case more overheads will be created for shifting the matrix . We can use 64 characters as a standard size of blocks which can improve performance. Suppose there is a plaintext which is divided into two blocks. So two random numbers are generated. Let the key be *CIPHER123* . The resulting matrix is shown in matrix 3.

Matrix 3 : 6x6 matrix(keyword :*CIPHER123*)

C	I	P	H	E	R
1	2	3	A	B	D
F	G	J	K	L	M
N	O	Q	S	T	U
V	W	X	Y	Z	0
4	5	6	7	8	9

Let the first random number be 3, so the shifted matrix is matrix 1 shown in matrix 3.1

Matrix 3.1: Shifted matrix 1

H	E	R	1	2	3
A	B	D	F	G	J
K	L	M	N	O	Q
S	T	U	V	W	X
Y	Z	0	4	5	6
7	8	9	C	I	P

It is a left shift in which the topmost left character is shifted to the bottommost right cell in the matrix. Matrix 1 will be used to encrypt the first block of the plaintext. Thereafter the second random number is used to shift the matrix 1 to produce matrix 2.

Let the second random number be 4. Matrix 2 is shown below in matrix 3.2:

Matrix 3.2 : Shifted matrix 2

2	3	A	B	D	F
G	J	K	L	M	N
O	Q	S	T	U	V
W	X	Y	Z	0	4
5	6	7	8	9	C
I	P	H	E	R	1

Given below are two message blocks of 32 characters each, that are to be encrypted:

i) **abcdef**12945ghijklmnopqrstu**vwxyz8**

ii) **abcdef**35297gijklmhqnoprstu**vwxyz8**

Now by using primary matrix shown in matrix 4, the above two messages are encrypted as:

i) **BDRILC**2345IOACKLMFOQ3XUHUN**WXYZ8E**

ii) **BDRILC**62D55K3FLMKRSOIQUHUN**WXYZ8E**

Matrix 4: Primary matrix

C	I	P	H	E	R
1	2	3	A	B	D
F	G	J	K	L	M
N	O	Q	S	T	U
V	W	X	Y	Z	0
4	5	6	7	8	9

Now by using Matrix 1 shown below in matrix 5.1, the above first message is encrypted as:

KE9FIB230CIOCAKBMNOQ3XAMUV**WXYT8E**

Matrix 5.1 Matrix 1

E	R	1	2	3	A
B	D	F	G	J	K
L	M	N	O	Q	S
T	U	V	W	X	Y
Z	0	4	5	6	7
8	9	C	I	P	H

Now by using Matrix 2 shown in matrix 5.2, the above second message is encrypted as:

BR9FCL62IR5KGPLDS9SOQIAMZM**WXYZ8E**

Matrix 5.2 : Matrix 2

R	1	2	3	A	B
D	F	G	J	K	L
M	N	O	Q	S	T
U	V	W	X	Y	Z
0	4	5	6	7	8
9	C	I	P	H	E

As shown in the above example, we have divided 64 characters plaintext into two blocks of 32 characters each and bold letters in the plain text shows that part which is same in both the blocks. When only primary matrix is used to encrypt both the texts then it generates same encrypted character for the same pair of plaintext characters.

Let the random numbers generated are 4 and 1 using SHA-1. The primary matrix is left shifted by 4 to get Matrix1. Now Matrix1 is used to encrypt the first block of 32 characters. Matrix1 is left shifted by 1 unit to get the Matrix2 which is used to encrypt the remaining 32 characters. By shifting the matrix, we are able to change the corresponding position of the characters(alphabets and numbers). Due to change in the matrix, the encrypted texts are different in both the blocks. This technique disguises the attacker and makes it highly secure against any form of cryptanalysis attack.

4. ANALYSIS OF PROPOSED METHOD

This proposed methodology increases the security of the data. Cryptanalysis of this proposed method is very tedious and difficult. The SHA-1 is used to generate random numbers. SHA-1 is considered to be very secure for generating pseudo random numbers. The random numbers can be generated by a third party and provided to the communicating parties at the time of encryption and decryption at the sending and the receiving end.

5. CONCLUSION

Proposed modified Block Playfair Cipher is highly secure as compare to other approaches. As it encrypts the plaintext in blocks uses different matrix for consecutive blocks, it is quite impossible for the cryptanalyst to generate the plaintext from the ciphertext. With each random shift the relative position of characters in the matrix change, which completely conceals the statistical structure of the plaintext which is the most peculiar property of this approach. As a result of these security features, this algorithm can be extensively used for sending and receiving messages with its confidentiality intact.

6. REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education.

[2] Security Aspects of the Extended Playfair Cipher ,Srivastava, S.S.; Gupta, N .; Communication Systems and network Technologies (CSNT), 2011

International Conference on Digital Object ,Publication Year: 2011 , Page(s): 144 - 147 ,IEEE Conferences

[3] Modified Version of Playfair Cipher Using Linear Feedback Shift Register Murali, P.; Senthilkumar, G.; Information Management and Engineering, 2009. ICIME '09. International Conference on Digital Object Identifier: Publication Year: 2009 , Page(s): 488 - 490 ,IEEE Conference

[4] Java Cryptography, Jonathan B. Knudsen First Edition May 1998 ISBN

[5] A Novel Approach to Security using Extended Playfair Cipher, International Journal of Computer Applications (0975 – 8887)Volume 20– No.6, April 2011 Shiv Shakti Srivastava, Nitin Gupta Department of Computer Science and Engineering Department of Computer Science and Engineering National Institute of Technology Hamirpur, India

[6] Johannes A.Buchmann, Introduction to Cryptography.Second Edition,Springer-Verlag NY, LLC,2001.

[7] Dhiren R.Patel, Information Security Theory and Practice.First Edition, Prentice-Hall of India Private Limited,2008

[8] Anne-Canteaut(Editor)"Ongoing Research Area in Symmentic Cryptography"ENCRYPT,2006.

[9] Schnier B, Applied cryptography:protocols,algorithms and source code in C.New York:John Wiley and sons,1996.