KEMENTERIAN PENDIDIKAN TINGGI

JOJAPS

eISSN 2504-8457

POLITEKNIK MALAYSIA PORT DICKSON

Journal Online Jaringan COT POLIPD (JOJAPS)

Modified Playfair Cipher Using Random Key Linear Congruent Method

Muhammad Syahrizal[1]*, Murdani[2], Surya Darma Nasution[3], Mesran[4], Robbi Rahim[5], Andysah Putera Utama Siahaan[6]

[1,2,3,4]*Department of Informatics Engineering, STMIK Budi Darma, Medan, Indonesia*
[5]*Department of Health Information, Akademi Perekam Medik dan Infokes Imelda, Medan, Indonesia*
[6]*Faculty of Computer Science, Universitas Pembangunan Panca Budi, Medan, Indonesia*
[5,6]*School of Computer and Communication Engineering, Universiti Malaysia Perlis, Kangar, Malaysia*

Abstract

The number of crimes that arise due to data does not have good security makes many users choose one or more cryptographic algorithms to secure data. The application of cryptographic algorithms is widely used such as to secure text data, secure messages on short message service (SMS), secure messages on chat applications, secure records on the database. Many modifications were made to obtain safer algorithms and in this study Playfair cipher which is a classical cryptographic algorithm modified by changing the key consisting of 25 characters to 255 characters and the key used to encode resulting from randomization using a linear congruent method. The result obtained is that the encoded text is hard to know and the key used is random, making it difficult to solve by cryptanalyst.

Key-word: Playfair Cipher, Cryptography, Text Message, Linear Congruent.

1. Introduction

Data security is very important in everyday life where the amount of data is very important and do not want to be known by others. Different types of cryptographic algorithms have been applied to secure data, but many of the cryptoanalysts have also successfully solved cryptographic algorithms. The type of cryptographic algorithm consists of classical cryptographic algorithms and modern cryptographic algorithms. The Classical cryptographic algorithm is rarely used because the algorithm is too easy and easy to solve. The modification of classical cryptographic algorithms is the best way to increase the level of security and make the cryptologist confused whether the cryptographic algorithm used is classic or modern. In previous research has also been done to modify the classic cryptographic algorithm of Playfair cipher where modification is done using Rectangular Matrix where lowercase and uppercase letters along with numbers or other characters can be used. Keywords can be single or multiple words or phrases where the number of non-duplicate characters can be a maximum of 90 characters. The modification of the Playfair cipher has also been done using a 7x4 matrix and using the symbol character. The modification of the algorithm can be applied to any language by simply taking a matrix of the right size, which can accommodate all the letters in that language.

2. Existing Playfair Cipher

The original Playfair Cipher uses 25 capital letters with the provision of a letter I = J or Q is omitted. Keywords for encoding are selected, and a 5 x 5 matrix is built by placing keywords without duplicate letters from left to right and from top to bottom. Other letters of the alphabet are then placed in the matrix. For example, if the key used choose BUDIDARMA as secret keyword matrix given in table 1.

Table 1: Traditional Playfair 5 x 5 matrix

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

The message to be secured is broken down by diagram or group of 2 letters. In case of duplicate letters in a diagram, one of the letters is used as padding and placed between letters. If the same number of odd character padding is applied at the end. Substitution occurs depending on the following three rules.

1. In case the diagram letters are on the same line, the letters to the right of each letter are taken. The wrapper occurs when one of the letters is in the last column.
2. If the letters in the same column the letters to the lower letters of each letter are taken. Again wrapping occurs in case any letter is in the last line
3. If the letters are not on the same row or column, a rectangle is created with letters and letters in the opposite corner taken.

In case of decryption, the reverse is done with ciphertext and we return plain text. For example, the plaintext used is KILLER and the keyword is BUDIDARMA then ciphertext is generated as follows:

1. Plaintext is converted to uppercase and then split into diagrams using X as a padding character. Diagram will be KI LX LH ER.
2. For the first diagram K and I are not on the same line thus using rule 3 will get LD.
3. The next diagram is LX which as before is not in the same row or column, using rule 3 we get YK.
4. Then LH lies on the same line so as to generate NK.
5. And the last diagram ER is in the same line and so we get FM. Thus the resulting ciphertext is LDYKNKFM.

3. Modified Playfair Cipher

Modifications are made to the Playfair cipher by using the 17x15 matrix where the columns and rows used are filled with characters having ASCII codes from 1 to 255. The key becomes changed as in table 2.

Table 2. Modified Playfair Cipher 17x15 Matrix from 1 to 255

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102
103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136
137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153
154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187
188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204
205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221
222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238
239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Table 3. Modified Playfair Cipher 17x15 Matrix Ascii Character

	┐	└	┘	|	–	•	◘			♂	◙		♫	※	┼	◄
↕	‼	¶	┴	┬	┤	↑	├	→	←						!	"
#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3
4	5	6	7	8	9	:	;	<	=	>	?	@	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	[	\	]	^	_	`	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	{	|	}	~	⌂	€		‚	ƒ	„	…	†	‡	ˆ
‰	Š	‹	Œ		Ž			‘	’	“	”	•	–	—	˜	™
š	›	œ		ž	Ÿ		¡	¢	£	¤	¥	¦	§	¨	©	ª
«	¬	-	®	¯	°	±	²	³	´	µ	¶	·	¸	¹	º	»
¼	½	¾	¿	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì
Í	Î	Ï	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý
Þ	ß	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î
ï	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

The use of a key table is to insert a keyword in the key table in Table II. Modifications are only made to the lock table, the use of rules of the Playfair cipher remains in use.

4. Random Key Linear Congruent Method

The use of a linear congruent method for generating random keys to encode plaintext on Playfair cipher.Linear Congruent Method (LCM) is one of the most common random number generator methods used to generate random numbers. The advantage of this method is the speed and ease of implementing it. One of the properties of this method is the repetition and combination of variables a, c and determines the result of randomization and it becomes the deficiency of this method. The following equation is the linear congruent method formula.

$$Xi + 1 = a.Xi + c \; mod \; m \qquad (1)$$

Where :

Xi + 1 = New random number.
Xi = Old random numbers or previous random numbers.
A = The number of constants of the multiplication.
C = Rate increase.
M = Module number.

The linear congruent method for generating random keys is to determine the values of variables a, c and m and in this case, the values a = 13, c = 7, m = 255 and the value of Xi (X0) are taken from the number of characters contained in the plaintext. Since the overall value of the key table is from 1 to 255 while the result of modulus 255 will likely get a value of 0 and will not get the value 255, so the result of randomization if there is a number 0 it will be added with number 1. It is done to avoid getting number 0.

For example :

Plaintext = KILLHER
Number of characters (X0) = 7
The number of Key Characters is assumed to be 8 and can be replaced as needed, then the key randomization process becomes:
X1 = a.X0 + c mod m = (13 *7)+7 mod 255= 98(b)
X2 = a.X1 + c mod m = (13 *98)+7 mod 255 = 6 (ACK)
X3 = a.X2 + c mod m = (13 *6)+7 mod 255 = 85 (U)
X4 = a.X3 + c mod m = (13 *85)+7 mod 255 = 92 (\ )
X5 = a.X4 + c mod m = (13 *92)+7 mod 255 = 183 (·)

X6 = a.X5 + c mod m = (13 *183)+7 mod 255 = 91 ([ )
X7 = a.X6 + c mod m = (13 *91)+7 mod 255 = 166 (¦)
X8 = a.X7 + c mod m = (13 *166)+7 mod 255 = 109 (m)

So the key table becomes:

Table 4. Key Table In ASCII Number Form

98	6	85	92	183	166	109	1	2	3	4	5	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62
63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	86	87	88	89	90	91	93	94	95	96	97	99
100	101	102	103	104	105	106	107	108	110	111	112	113	114	115	116	117
118	119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134
135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151
152	153	154	155	156	157	158	159	160	161	162	163	164	165	167	168	169
170	171	172	173	174	175	176	177	178	179	180	181	182	184	185	186	187
188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204
205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221
222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238
239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

Table 5. Key Table In ASCII Character Form

b	–	U	\	·	¦	m		┐	└	┘	|	•	◘			♪
◙		♫	▒	┼	◄	↕	‼	¶	┴	┬	┤	↑	├	→	←	
				!	"	#	$	%	&	'	(	)	*	+	,	-
.	/	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>
?	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	V	W	X	Y	Z	[	]	^	_	`	a	c
d	e	f	g	h	i	j	k	l	n	o	p	q	r	s	t	u
v	w	x	y	z	{	|	}	~	▯	€		‚	ƒ	„	…	†
‡	ˆ	‰	Š	‹	Œ		Ž			‘	’	“	”	•	–	—
˜	™	š	›	œ		ž	Ÿ		¡	¢	£	¤	¥	§	¨	©
ª	«	¬	-	®	¯	°	±	²	³	´	µ	¶	¸	¹	º	»
¼	½	¾	¿	À	Á	Â	Ã	Ä	Å	Æ	Ç	È	É	Ê	Ë	Ì
Í	Î	Ï	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	×	Ø	Ù	Ú	Û	Ü	Ý
Þ	ß	à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î
ï	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù	ú	û	ü	ý	þ	ÿ

Based on the key table and the plaintext used is KILL HER. And the keyword is: bACKU\[¦m So the ciphertext is generated as follows:

1. Plaintext is converted to uppercase and then split into diagrams using X as the padding character. Diagram will be KI LX LH ER.
2. For the first diagram K and I lie on the same row to produce LJ.
3. The next diagram is the LX is not in the same row or column, using rule 3 we get _F.
4. Then LH lies on the same line so as to produce MI.
5. And the last diagram ER by using rule 3 so get WA. Thus the resulting ciphertext is LJLX_FMIWA.

5. Conclusion

In this paper, we can generate a way to secure the text with a random key with more characters than the original Playfair cipher algorithm. The use of 255 characters makes the resulting ciphertext variations. The result obtained is that the encoded text is hard to know and the key used is random, making it difficult to solve by cryptanalyst.

References

Alam, A., et al. (2013). "Universal Playfair Cipher Using MXN Matrix." International Journal of Advanced Computer Science 1(3): 113-117.
Basu, S. and U. K. Ray (2012). "Modified Playfair Cipher using Rectangular Matrix." International Journal of Computer Applications 46(9): 28-30.
Fitriani, W., et al. (2017). "Vernam Encypted Text in End of File Hiding Steganography Technique." International Journal of Recent Trends in Engineering & Research 3(7): 214-219.
Hanosh, O. N. A. and B. Salim (2013). "11 × 11 Playfair Cipher based on a Cascade of LFSRs." IOSR Journal of Computer Engineering 12(1): 29-35.
Iqbal, M., et al. (2016). "SMS Encryption Using One-Time Pad Cipher." IOSR Journal of Computer Engineering 18(6).
Kahate, A. Cryptography and Network Security, Tata McGraw-Hill Publishing.
Kurnia, D., et al. (2017). "RSA 32-bit Implementation Technique." International Journal of Recent Trends in Engineering & Research 3(7): 279-284.
Nasution, S. D. (2013). "Penerapan Metode Linear Kongruen dan Algoritma." Pelita Inform 4(1): 94-102.
Oktaviana, B. and A. P. U. Siahaan (2016). "Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography." IOSR Journal of Computer Engineering 18(4): 26-29.
Ramadhan, Z., et al. (2017). "The Utilization of Cloud Computing as Virtual Machine." International Journal of Recent Trends in Engineering & Research 3(7): 396-399.
Sari, R. D., et al. (2017). "A Review of IP and MAC Address Filtering in Wireless Network Security." International Journal of Scientific Research in Science and Technology 3(6): 470-473.
Siahaan, A. P. U. (2016). "Rail Fence Cryptography in Securing Information." International Journal of Scientific & Engineering Research 7(7): 535-538.
Sumartono, I., et al. (2016). "Base64 Character Encoding and Decoding Modeling." International Journal of Recent Trends in Engineering & Research 2(12): 63-68.
Tasril, V., et al. (2017). "Threats of Computer System and its Prevention." International Journal of Scientific Research in Science and Technology 3(6): 448-451.
Tunga, H., et al. (2014). "Novel Modified Playfair Cipher using a SquareMatrix." International Journal of Computer Applications 101(12): 16-21.