Implementation of Super Playfair in Messaging

Andysah Putera Utama Siahaan[1,3], Mesran Mesran[2], Imam Solihin[2]
[1]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Department of Computer Informatics, STMIK Budi Darma, Indonesia
[3]School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia

andiesiahaan@gmail.com, mesran.skom.mkom@gmail.com

ABSTRACT

Data is the essential thing in the world of communication. Text messaging is a way of communicating that is sent in digital form. This message is very widely used in electronic media such as short message service. This message was sent through the service provider. Messages sent are unsafe and can be intercepted at the time of submission. Message delivery needs to apply cryptographic algorithms to text messages sent using encryption and decryption techniques. Super Playfair cipher and two square cipher algorithms are a development of Playfair cipher method. This method is a quite complicated way of solving it than other classical methods. These methods belong to classical cryptographic algorithms that use substitution encoding techniques and character transitions that use a symmetric key in the process of encryption and decryption.

Keywords: *Cryptography, Super Playfair, Two Square, Symmetric Key*

1. INTRODUCTION

Data security is very important and should be applied in the delivery of information [1][2][3]. Text messages are electronic writings that practice making or sending short messages from two or more phones to communicate and exchange information [4][5]. The use of SMS is prevalent today used as one of the smooth and fast communication tools. Communication requires a fast and precise tool and search system [6][7][8][9]. However, the distribution of message content is very vulnerable to interference or theft by wild parties [10]. Therefore, messages that will be sent need extra security to avoid the theft or editing of the message content before it reaches the recipient of the message because the contents of a plaintext message can be read by anyone who has access to the contents of the message.

Moreover, mobile phones have now developed into smartphones that have high capabilities [11], and often have a function as a computer [12]. Smartphones are currently mostly run by using the Android operating system. Android is a Google-made operating system that is open source. It makes more and more developers develop applications on Android. Android application created with JAVA programming language and one of the most popular and widely used Integrated Development Environment is Eclipse. Also, Android requires Software Development Kit as a device emulator for application compiled. Cryptography is a science and art to keep messages safe [13][14]. The process is done to secure a plaintext into ciphertext. It

is a message that cannot be read. The reverse process easily for converting ciphertext to plaintext is called decryption [15].

In its definition, Super-Playfair is a variant of the Playfair Cipher algorithm by altering the 5x5 cube rules contained therein, to then be performed Super-Encryption. Super-Encryption itself is doing the first encryption with simple substitution Cipher; then the result is encrypted again with Cipher transposition. The modification process to Playfair Cipher is expected to strengthen this algorithm. The two square cipher was developed to have a classical system stronger than the Playfair cipher and less practical than the Foursquare cipher. It is a graphics system, where two plaintexts are replaced with two ciphertext letters in each encoding. It comprises 25 squares either next to each other (horizontally Two square) or on top of each other (vertical Two square). Typically, both boxes containing mixed order should use two different keywords [16].

2. THEORIES

2.1 Cryptography

Cryptography is the science of text modification becoming unreadable. Cryptography has patterns like in steganography and image processing [17][18]. Data security is required because of the large number of cyber crimes [19]. It is called the encryption technique where plaintext is randomized using a key to be ciphertext [20][21]. Cryptography can result in greater or compressed ciphertext results. Compression is also a cryptographic model that compresses the message content [22][23]. If someone does not have a decryption key, then the person can not understand the contents of the text [24]. Decryption is the process of returning ciphertext to plaintext. The probability of retrieving the original script by someone who has not had a decryption key is very small [25]. The encryption technique used in classical cryptography is symmetric encryption where the decryption key is the same as the encryption key. For public key cryptography, an asymmetric encryption technique is required where the decryption key is not the same as the encryption key [26][27]. Encryption, decryption and key creation for asymmetric encryption techniques require more intensive computation than symmetric encryption since asymmetric encryption uses huge numbers.

2.2 Playfair Cipher

Playfair Cipher was invented by Sir Charles Wheatstone (1802-1875) in 1854, and popularized by Baron Lyon Playfair (1819-1898), whose name is immortalized for this algorithm. Although the Playfair algorithm is already unsafe for the usefulness of the world today [28][29]. Playfair cipher is widely used and quite useful in its era. British soldiers first used Playfair ciphers during the Boer war and still used in World War I. Playfair Cipher is a classical cryptographic algorithm that belongs to a polygram cipher where plaintext is converted to a polygram form, and a decryption encryption process is performed for the polygraph [30]. The cryptographic key is 25 letters arranged in a 5x5 bundle by removing the letter J from the alphabet. The key possibility is 25. The key arrangement inside the square extends by adding the sixth and sixth rows. The sixth base is the first line, while the sixth column contains the first column. In general, the key used is a series of words that are easy to understand.

3. RESULT AND DISCUSSION

Text messages to be encrypted are capital letters. The encryption process begins by using Super Playfair Cipher algorithm and then re-encrypted using the Two Square Cipher algorithm to get the ciphertext.

3.1 Encryption Process

Encryption process using super playfair cipher algorithm:

```
Plaintext  :  STMIK BUDIDARMA MEDAN
Key        :  IMAM SOLIHIN
```

a. Change plaintext to bigram form: ST MI KB UD ID AR MA ME DA NZ
b. Eliminate any of the letters J, Q, or Y in the square according to which there are many locks. The key does not contain the letter so the letter "J" will be omitted to form a square.

   The key square can be seen in the following illustration.

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

   Encryption for the first bigram is ST, the result is BY.

c. Make a square change to the key.

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

   Encryption for the second bigram is MI, the result of ciphertext is AM.

d. Make a square change to the key.

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

Y	Z	V	W	X	Y
S	O	I	M	A	

Encryption for the third bigram is KB, the ciphertext is GC.

e. Make a square change to the key.

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

Encryption for the fourth bigram is UD, the result of cipherteks is PK.

f. Make a square change to the key.

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

Encryption for the fifth bigram ID, the result of cipherteks is LP.

g. Make a square change to the key.

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

Encryption for the sixth bigram is AR, the result of cipherteks is NX.

h. Make a square change to the key.

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

O	I	M	A	S	

Encryption for the seventh bigram is MA, cipherteks result is US.

i. Make a square change to the key.

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

Encryption to the eighth bigram is ME, the result of ciphertext is HQ.

j. Make a square change to the key.

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

Encryption for the ninth bigram is DA, the result of cipherteks is FI.

k. Make a square change to the key.

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

Encryption for the tenth bigram is NZ, the ciphertext is CX.

The ciphertext result is BY AM GC PK LP NX AS HQ FI CX. After completion of encryption using the Playfair cipher variant, here is a super encryption, by performing a transposition cipher according to the key length.

The key length is 11, K = 11
B Y A M G C P K L P N
X A S H Q F L C X X X

The final chipertext of encryption super playfair cipher algorithm is BXYAASMHGQCFPLKCLXPXXX

3.2 Decryption Process

Decryption is a reverse process of encryption because at the time of encryption using super Playfair. This decryption process starts from the algorithm that was last used at the time of encryption. The ciphertext of the super playfair cipher is then decrypted as seen in the following illustration.

```
Ciphertext:  BXYAASMHGQCFPLKCLXPXXX
Key        :  IMAM SOLIHIN
```

a. Decrypt with the transition technique (flipping the row into columns according to key length) because the key length is 11; K = 11

   BXYAASMHGQCFPIKCLXPXXX
   B Y A M G C P K L P
   X A S H Q F C X X X

   The decryption is BYAMGCPKLPNXASHQFICXXX

b. Eliminate the addition of letters when transposition techniques, such as (double XX letters located at the end). BYAMGCPKLPNXASHQFICXXX become BYAMGCPKLPNXASHQFICX then change to bigram BY AM GC PK LP NX AS HQ FI CX.

c. Form key squares by removing any of the letters J, Q, or Y in the square according to which there are many keys, since the key does not contain the letter then the letter "J" which will be omitted to form the square. The result of the key square is as follows.

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

   Decryption for the first bigram is BY, the result of plaintext is ST.

d. Make a square change to the key.

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

O	I	M	A	S	

Decryption for the second bigram is AM, the result of plaintext is MI.

e. Make a square change to the key.

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

Decryption for the first bigram is CG, the result of plaintext is KB.

f. Make a square change to the key.

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

Decryption for the first bigram is PK, the result of plaintext is UD.

g. Make a square change to the key.

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

Decryption for the first bigram is LP, the result of plaintext is ID.

h. Make a square change to the key.

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

Decryption for the first bigram is NX, the result of plaintext is AR.

i. Make a square change to the key.

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

Decryption for the first bigram is AS, the result of plaintext is MA.

j. Make a square change to the key.

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

Decryption for the first bigram is HQ, the result of plaintext is ME.

k. Make a square change to the key.

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

Decryption for the first bigram is FI, the result of plaintext is DA.

l. Make a square change to the key.

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

Decryption for the first bigram is CX, the result of plaintext is NZ.

The result of plaintext is ST MI KB UD ID AR MA ME DA NZ. It becomes "STMIK BUDIDARMA MEDAN."

4. CONCLUSION

Based on the results of research, experimental execution and analysis and discussion can be taken a conclusion that the use of playfair cipher method on text encoding is good enough because the key matrix used has a small possibility to be solved. Super Playfair cipher is best used for symmetric cryptography type. The bigram substitution technique on the key matrix has a small chance to solve. Each bigram change, the matrix pattern changes to the key. This manjadikan this method is very difficult to solve.

REFERENCES

[1] A. P. U. Siahaan, "Rail Fence Cryptography in Securing Information."

[2] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, *Handbook of Applied Cryptography*, 1st ed. Florida: CRC Press, Inc. Boca Raton, 1996.

[3] V. Tasril, M. B. Ginting, Mardiana, and A. P. U. Siahaan, "Threats of Computer System and its Prevention," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 448–451, 2017.

[4] S. Aryza, M. Irwanto, Z. Lubis, A. P. U. Siahaan, R. Rahim, and M. Furqan, "A Novelty Design of Minimization of Electrical Losses in A Vector Controlled Induction Machine Drive," in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 300, no. 1.

[5] R. Rahim, Mesran, A. P. U. Siahaan, and S. Aryza, "Composite Performance Index for Student Admission," *Int. J. Res. Sci. Eng.*, vol. 3, no. 3, pp. 68–74, 2017.

[6] Z. Sitorus and A. P. U. Siahaan, "Heuristic Programming in Scheduling Problem Using A* Algorithm," *IOSR J. Comput. Eng.*, vol. 18, no. 5, pp. 71–79, 2016.

[7] A. P. U. Siahaan, "A Three-Layer Visual Hash Function Using Adler-32," *Int. J. Comput. Sci. Softw. Eng.*, vol. 5, no. 7, pp. 142–147, 2016.

[8] A. P. U. Siahaan, "Adler-32 Integrity Validation in 24bit Color Image."

[9] R. Rahim *et al.*, "Searching Process with Raita Algorithm and its Application," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, pp. 1–7, 2018.

[10] A. P. U. Siahaan and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016.

[11] R. Meiyanti, A. Subandi, N. Fuqara, M. A. Budiman, and A. P. U. Siahaan, "The Recognition of Female Voice Based on Voice Registers in Singing Techniques in Real-Time using Hankel Transform Method and Macdonald Function," *J. Phys. Conf. Ser.*, vol. 978, no. 1, pp. 1–6, 2018.

[12] M. Iqbal, M. A. S. Pane, and A. P. U. Siahaan, "SMS Encryption Using One-Time Pad Cipher," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 54–58, 2016.

[13] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, pp. 1–5, 2018.

[14] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique."

[15] J. Sasongko, "Pengamanan Data Informasi menggunakan Kriptografi Klasik," *J. Teknol. Inf. Din.*, vol. 10, no. 3, pp. 160–167, 2005.

[16] D. Bishop, *Introduction to Cryptography*. Jones and Batrlet Publisher, 2002.

[17] N. A. Putri, A. P. U. Siahaan, F. Wadly, and Muslim, "Image Similarity Test Using Eigenface Calculation," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 510–515, 2017.

[18] A. P. U. Siahaan, "High Complexity Bit-Plane Security Enchancement in BPCS Steganography," *Int. J. Comput. Appl.*, vol. 148, no. 3, pp. 17–22, 2016.
[19] A. P. U. Siahaan, "Pelanggaran Cybercrime dan Kekuatan Yuridiksi di Indonesia," *J. Tek. dan Inform.*, vol. 5, no. 1, pp. 6–9, 2018.
[20] Haryanto, A. P. U. Siahaan, R. Rahim, and Mesran, "Internet Protocol Security as the Network Cryptography System," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 223–226, 2017.
[21] Hariyanto and A. P. U. Siahaan, "Intrusion Detection System in Network Forensic Analysis and," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 115–121, 2016.
[22] Suherman and A. P. U. Siahaan, "Huffman Text Compression Technique," *Int. J. Comput. Sci. Enginee ring*, vol. 3, no. 8, pp. 103–108, 2016.
[23] L. Marlina, A. P. U. Siahaan, H. Kurniawan, and I. Sulistianingsih, "Data Compression Using Elias Delta Code," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 8, pp. 210–217, Aug. 2017.
[24] M. D. L. Siahaan, M. S. Panjaitan, and A. P. U. Siahaan, "MikroTik Bandwidth Management to Gain the Users Prosperity Prevalent," *Int. J. Eng. Trends Technol.*, vol. 42, no. 5, pp. 218–222, 2016.
[25] A. Lubis and A. P. U. Siahaan, "Network Forensic Application in General Cases," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 41–44, 2016.
[26] D. Kurnia, H. Dafitri, and A. P. U. Siahaan, "RSA 32-bit Implementation Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 279–284, 2017.
[27] D. Kurnia, H. Dafitri, Sugianto, Mardiana, and A. P. U. Siahaan, "RSA 32-bit Implementation Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 279–284, Jul. 2017.
[28] I. Sumartono, A. P. U. Siahaan, and N. Mayasari, "An Overview of the RC4 Algorithm," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 67–73, 2016.
[29] R. D. Sari, Supiyandi, A. P. U. Siahaan, M. Muttaqin, and R. B. Ginting, "A Review of IP and MAC Address Filtering in Wireless Network Security," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 6, pp. 470–473, 2017.
[30] M. Syahrizal, M. Murdani, S. D. Nasution, M. Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," *J. Online Jar. COT POLIPD*, vol. 10, no. 2, pp. 45–49, 2017.