PROC. INTERNAT. CONF. SCI. ENGIN.
Volume 3, April 2020 | Pages: 273-277

ISSN 2597-5250
E-ISSN 2598-232X

How Can Playfair Cipher Secure Data?

Luthfi Nur Azizah
Graduate Program of Mathematics Education, Universitas Negeri Yogyakarta, Indonesia
Jl. Colombo No. 1 Depok, Caturtunggal, Sleman,55281, Yogyakarta, Indonesia.
Email: luthfinurazizah.2017@student.uny.ac.id

Abstract. Cryptography plays an important role in the digital world today. Information can be mathematically secured by the message sender with a key. The intended sender's privacy and recipient's information will be protected from eavesdroppers. The purpose of this paper is to find out how to secure data using a playfair cipher with a 16 X 16 matrix. This algorithm will provide the power to playfair cipher. The encryption and decryption process in cryptography uses keywords that have been agreed upon by the sender and recipient of the message. Entries of this matrix are large and small alphabet letters, numerical characters, and other special characters to construct the contents of the matrix. The characters refer to ASCII from 0 to 255.

Keywords: Playfair Cipher, Enkripsi.

INTRODUCTION

The rapid development of the world will be accompanied by the advancement of information technology. Various kinds of information are easily accessed anytime, anywhere. Because there is a lot of ease in accessing information, a security is needed to access the information. This security serves to prevent the arrival of information to unauthorized hands. Based on this, information security is now an important issue in data storage and transmission (Setyaningsih, Iswahyudi, & Widyastuti, 2011).

There are many security methods that are used to maintain good communication, such as by providing passwords, encrypting message content and other methods to strengthen security. Sending data and storing data through electronic media requires a process that can guarantee the security and integrity of the data sent. The data must remain confidential during transmission and must remain intact upon receipt at the destination. To fulfill this, an encryption process is carried out on the data to be sent.

The encoding process is done by using cryptography. Cryptography is the art of hiding messages. The existence of cryptographic algorithms is to avoid threats to confidentiality and the availability of integrity (Choudhary, Gupta, & Singh, 2013). Cryptography encompasses the process of transforming information into an incomprehensible form, so unauthorized people are unlikely to understand. This transformation must take place in two directions, so that people who intend to read the information can understand the meaning of the transformation formation. The transformation nhgnnhprocess consists of encryption and decryption. The flow or series of these processes can be seen in the following figure 1.

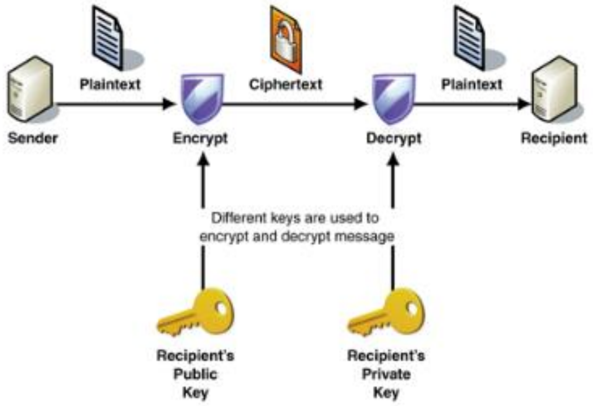

Figure 1. Encryption and decryption process.

Plaintext is data or information that can be understood, that is original text and needs to be transferred securely to the recipient of the message. This plaintext is the main input to the encryption algorithm. Furthermore, the secret key is the main component used to convert plaintext to ciphertext, which is a form that cannot be understood and hidden in a certain way. The process of converting plaintext into ciphertext is called encryption.

Encryption algorithms are classified into two groups namely Symmetric-key (also called secret-key) and Asymmetric (also called public key) (Singh, 2013). In symmetric cryptography a single key is shared between the sender and receiver. The sender uses a shared key and an encryption algorithm to encrypt the message. The recipient uses the shared key and decrypts the algorithm to decrypt the message. Whereas in Asymmetric Key Cryptography each user is given a pair of keys, a public key and a private key (Alam, Khalid, & Salam, 2013). So, the difference between these two algorithms lies in using the key used to encrypt data.

The output of the encryption process where we take the plaintext and secret key as input and are processed by the encryption algorithm is ciphertext. Ciphertext can be understood as a random piece of text that has useful information in a confidential form (Choudhary et al., 2013). Encryption is done at the time of delivery by changing the original data into confidential data while decryption is done at the time of receipt by changing the confidential data into original data. So the data sent during the sending process is confidential data, so the original data cannot be known by unauthorized parties.

Original data can only be known by the recipient by using a secret key. There are several encryption algorithms that can be used to secure information. Cryptographic algorithm consists of two namely classical and modern cryptographic algorithms. Classical cryptographic algorithms are used since before the computerization era and most use symmetric key techniques. The method of hiding the message is by substitution or transposition techniques or both. Examples of classic cryptographic algorithms are Caesar Cipher, Vigenere Cipher, and Hill Cipher. While modern cryptographic algorithms are MD5, RC4, AES and others (Sumandri, 2017).

The classic cryptographic algorithm basically consists of a substitution cipher and a transposition cipher, where the keys for encryption and decryption are the same. There are so many examples of classical cryptographic algorithms such as Caesar Cipher, Vigenere Cipher, and Playfair Chipher. However, these algorithms are still vulnerable to attack and have many weaknesses. Classical cryptographic algorithms can generally be defeated by performing frequency analysis methods or guess techniques. With this weakness that gave birth to the birth of modern cryptographic algorithms. Although there are many weaknesses of the classical cryptographic algorithm, classical cryptography can be used as a source of understanding of the basic concepts of cryptography, and from these weaknesses we get a new algorithm that is more secure against existing attacks.This paper is a literature study from several sources about Playfair Cipher in securing data. The purpose of this paper is to find out how to secure data using a playfair cipher with a 16 X 16 matrix.

MATERIALS AND METHODS

Playfair Cipher

Playfair is a substitution cipher. Playfair cipher was originally developed by Charles Wheatstone in 1854 [4]. But Lord Playfair promotes the use of this algorithm or method so called the Playfair Cipher(Basu & Kumar Ray, 2012). This method was used by the British in the Second Boer War and in World War I. It was also used by Australians and Germans during World War II. Playfair is quite easy to use and is used to handle secrets but is not so important. When enemy cryptanalysts can damage messages, that information will not be useful to them. Between February 1941 and September 1945, the New Zealand Government used it for communication between New Zealand, the Chatham Islands and the Pacific Islands(Basu & Kumar Ray, 2012).

Playfair Cipher is a classic cryptographic algorithm that is included in the polygram cipher, where plaintext is converted into polygram form and the encryption decryption process is performed for the polygram(Basu & Kumar Ray, 2012). The cryptographic key is 25 letters arranged in a 5x5 square table by removing the letter J from the alphabet. Possible key is 25!. The arrangement of keys in the square is expanded by adding the sixth column and the sixth row. The sixth base contains the first row, while the sixth column contains the first column. In general, the key used is a series of words that are easy to understand.

Playfair Cipher Algorithm with 5 X 5 Matrix

The Playfair Cipher algorithm is based on the use of a 5 X 5 matrix as letters constructed using keywords (Ravindra Babu, Uday Kumar, Vinay Babu, Aditya, & Komuraiah, 2011). The cryptographic key is 25 letters arranged in a 5x5 square by removing the letter J from the alphabet. In general, the key used is a series of words that are easy to understand.The message to be encrypted is arranged in advance, with the following rules:

1. Change the letter with J (if any) with the letter I
2. Write the message in pairs of letters
3. Do not have the same pair of letters. If there is, insert Z in the middle
4. If the number of letters is odd, add an X at the end

Encryption algorithm as follows:

1. If there are two letters in the same key line, then each letter is replaced by the letter to the right (in the expanded key)
2. If two letters are in the same key column, then each letter is replaced by a letter below it (in the expanded key)
3. If two letters are not in the same row or the same column, then the first letter is replaced by the letter at the intersection of the first letter's row with the second letter column
4. The second letter is replaced by a letter at the fourth vertex of the rectangle formed from the 3 letters used so far

Examples of Using the Playfair Cipher Algorithm on a 5 x 5 Matrix

First make the Playfair Cipher algorithm key

Keywords: **PLAYFAIR CIPHER**

1. Arrange the letters first, the letters that have been mentioned are no longer written PLAYFIRCHE then if there is a letter J then it is replaced with the letter I.

2. Next, add the remaining letters of the alphabet that are not on the previous key BDGKMNOQSTUVWXZ, so that it becomes PLAYFIRCHEBDGKMNOQSTUVWXZ.
3. Enter into the square matrix

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

4. Then the key is expanded to enter the encryption process
5. Plaintext: LUTHFI NUR AZIZAH
    - Eliminate all characters that are not letters of the alphabet
    - Because there is no letter J, do the letter pairs immediately
    - If there are the same pair of letters, insert the letter Z
    - If it has been paired, it is obtained
    - LU TH FI NU RA ZI ZA HX
6. After pairing, encrypt each pair using the key.

LU encryption to PV

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

TH encryption to SE

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

FI encryption to PE

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

NU encryption to UP

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

RA encryption to CL

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

ZA encryption to WF

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

ZI encryption to UE

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

HX encryption to KY

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

After the encryption process is complete, the encryption results are as follows:
Plainteks : **LU TH FI NU RA ZI ZA HX**
Cipher : **PV SE PE UP CL UE WF KY**

There are some limitations to the 5 x 5 matrix cipher algorithm which is as follows:

1. Regard the letters I and J as one character.
2. 26 letters can only be taken as keywords without duplicates.
3. The space between two words in the text is not considered as one character.
4. Cannot use numbers or special characters.
5. Can only use uppercase letters.

Additional X letters are added when the word plaintext consists of an odd number of characters. In the decryption process X is ignored. X is a valid character and so it can be confusing because it can be part of the plaintext, so we can't just deleteX in the decryption process.

The Playfair Cipher method can be modified by increasing the size of the matrix. For example with an enlarged square matrix size. In addition, it can be changed to the size of 6 x 6, 7 x 4, 10 x 9, or 16 x 16. For example, at size 7 x 4, the Playfair cipher matrix of any word without repetition of letters can be chosen as a keyword. The remaining space is filled according to the rest of the letters. the second last column is filled with the symbol "*" and the last column is filled with the symbol "#". However, the change in matrix size still has many limitations. So the size that might be able to enter all possible characters into the matrix is the size of 16 x 16.

In this method, in addition to the letters of the alphabet there are also numbers and symbols that can be encrypted. The American Standard Code or symbol used for Information Exchange is referred to as the American Standard Code for Information Interchange. ASCII is often found on computer keyboards or digital instruments. The number of ASCII codes is 255 codes. ASCII code 0..127 is ASCII code for text manipulation while ASCII code 128..255 is ASCII code for graphic manipulation. ASCII codes are numerical representations of characters such as ‘a’ or ‘@’ or non-printed characters, for example misalnya Σ ’. The table below shows the ASCII characters including 32 non-printed characters.

RESULTS AND DISCUSSION

The Playfair Cipher Algorithm on A 16 x 16 Matrix

This algorithm can accept Plaintext containing Alphabets (upper and lower case), Numbers and special characters. So users can easily encrypt combinations of letters, numbers and characters efficiently. To encrypt plaintext, the 5x5 rule is followed by the following modifications:

1. When repeating the plaintext character that is in the same pair, the first character is replaced by the character on the right, with the first element of the line in a circle following the last one. The second character is replaced by the character on the left, with the last element of the line following the first.
2. If a word consists of an odd number of characters, then add the "Null" character to complete the pair, because the "Null" character cannot affect the Plaintext at the time of parsing.

Algorithm:

1. Read keywords.
2. Eliminate repeated characters in keywords.
3. Build a matrix by filling in keyword characters from left to right and top to bottom.
4. Fill in the matrix entries with the remaining characters from ASCII valued from 0 to 255.
5. Read the plaintext.
6. Divide the plaintext into a pair of characters.
7. Add the "Null" character when the number of characters in the message is odd.
8. Conversion process:
   a. If the plaintext pair is on the same line then the matrix is replaced by the character to the right, with the first element of the line following the left.
   b. If the plaintext pair is in the same column of the matrix it is replaced by the characters below it, with the top row elements following in the last circle.
   c. If the plaintext pairs are the same, the first character is replaced by the character on the right. The second character is replaced by the character on the left.
   d. If plaintext pairs appear on different rows and columns, each plaintext character is replaced by a character that is located in itself row and column occupied by other plaintext characters.

The Playfair algorithm is based on the use of a 16x16 character matrix built using keywords. The matrix is constructed by filling in keyword characters (minus duplicates) from left to right and from top to bottom. Then fill in the remaining characters in ascending order from ASCII Values 0 to 255.

Example:

Keywords : Playfair. (Sample)
Plaintext : American.Online270@gmail.com

16x16 Playfair Matrix Table

P	l	a	y	f	i	r	.	(	S	m	p	e	)	NUL	☺
☻	♥	♦	♣	♠	•	◘	○	◙	♂	♀	♪	♫	☼	►	◄
↕	‼	¶	§	▬	↨	↑	↓	→	←	∟	↔	▲	▼	Space	!
“	#	$	%	&	‘	*	+	,	-	/	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	Q	R	T	U	V
W	X	Y	Z	[	\	]	^	_	`	b	c	d	g	h	j
k	n	o	q	s	t	u	v	w	x	z	{	|	}	~	DEL
Ç	ü	é	â	ä	À	å	ç	ê	ë	è	ï	î	ì	Ä	Å
É	æ	Æ	ô	ö	Ò	û	ù	ÿ	Ö	Ü	¢	£	¥	₧	ƒ
á	í	ó	ú	ñ	Ñ	ª	º	¿	⌐	¬	½	¼	¡	«	»
░	▒	▓	│	┤	╡	╢	╖	╕	╣	║	╗	╝	╜	╛	┐
└	┴	┬	├	─	┼	╞	╟	╚	╔	╩	╦	╠	═	╬	╧
╨	╤	╥	╙	╘	╒	╓	╫	╪	┘	┌	█	▄	▌	▐	▀
α	ß	Γ	π	Σ	Σ	µ	T	Φ	Θ	Ω	δ	∞	φ	ε	∩
≡	±	≥	≤	⌠	⌡	÷	≈	°	·	·	√	ⁿ	²	■	

Chipertext : ?e).p\lomLü♥lt)1$@Bcyerap^az

Am	:	?e	e2	:	)1
er	:	).	70	:	$@
ic	:	p\	@g	:	Bc
an	:	lo	ma	:	ye
.O	:	mL	il	:	ra
nl	:	ü♥	.c	:	p^
in	:	lt	om	:	az

The advantage of using Playfair with a 16 x 16 matrix is as follows.

1. Allows more than 36 characters as keywords.
2. Consider the space between two words in the plaintext as one character.
3. Users can easily encrypt and decrypt combinations of letters, numbers and special characters efficiently.
4. Letters, numbers and special characters are used to construct 16x16 matrices.
5. The letters I and J are considered as two different letters.
6. To compare with the previous algorithm, here the length of the keyword can be longer, so it is very difficult to find the Plaintext of the Ciphertext without knowing the key.
7. This algorithm adds the Null character to complete the pair, because the "Null" character cannot affect the plaintext at the end of a word or sentence.

CONCLUSIONS

Playfair cipher is a classic cryptographic algorithm that uses symmetric key techniques. This algorithm is based on the use of 5 X 5 matrix letters that are built using keywords. However, this algorithm still has limitations, one of which is that it cannot generate lowercase characters, numeric characters, and other characters. So that the matrix development needs to be done, it is 16 x

16. This algorithm uses ASCII code as the entry of the matrix. Election of complicated keywords can produce cipher text that is not easy to guess. In addition, to further enhance data security, it can be done by modifying the size of the matrix. Future enhancements can be made by creating two different keys so that they can be more safely applied for encryption and decryption.

REFERENCES

Alam, A. A., Khalid, B. S., & Salam, C. M. (2013). A Modified Version of Playfair Cipher Using 7×4 Matrix. *International Journal of Computer Theory and Engineering*, *5*(4), 626–628. https://doi.org/10.7763/IJCTE.2013.V5.762

Basu, S., & Kumar Ray, U. (2012). Modified Playfair Cipher using Rectangular Matrix. *International Journal of Computer Applications*, *46*(9), 975–8887. https://doi.org/10.5120/6939-9332

Choudhary, J., Gupta, R. K., & Singh, S. (2013). A Survey of Existing Playfair Ciphers. *International Journal of Engineering and Advanced Technology*, *2*(4), 658–659.

Ravindra Babu, K., Uday Kumar, S., Vinay Babu, A., Aditya, I. V. N. ., & Komuraiah, P. (2011). An Extension to Traditional Playfair Cryptographic Method. *International Journal of Computer Applications*, *17*(5), 34–36. https://doi.org/10.5120/2213-2814

Setyaningsih, E., Iswahyudi, C., & Widyastuti, N. (2011). Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra. *Prosiding Seminar Nasional Sistem & Teknologi Informasi (SNASTI) 2011*, ISLP 7-ISLP 10.

Singh, G. & S. (2013). A Study of Encryption Algorithms (RSA , DES , 3DES and AES) for Information Security. *International Journal of Computer Applications*, *67*(19), 33–38. Retrieved from https://pdfs.semanticscholar.org/187d/26258dc57d794ce4badb094e64cf8d3f7d88.pdf

Sumandri. (2017). Studi Model Algoritma Kriptografi Klasik dan Modern. *SEMINAR MATEMATIKA DAN PENDIDIKAN MATEMATIKA UNY*, 265–272.

THIS PAGE INTENTIONALLY LEFT BLANK