http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 10, No 02 September 2020
E-ISSN.2797-7889, P-ISSN.2089-3329

Analysis and Implementation of PlayFair Chipper Algorithm in Text Data Encoding Process

Pristiwanto[1], Heri Sunandar[2], Berto Nadeak[3]
Teknik Informatika, Universitas Budidarma Medan
Email: wanto97@gmail.com[1], herinandar44@gmail.com[2], nadeak85@gmail.com[3]

Keywords

Playfair Cipher
Keyboard
Encryption
Decryption

Abstract. This research discusses the implementation of Playfair Cipher to encode text data. Playfair Cipher is one of the classic cryptographic algorithms that use symmetry keys. Originally invented by Sir Charles Wheatstone and Baron Lyon Playfair, the algorithm used a 5x5 keyboard to encrypt and decrypt. The process of encryption and decryption is done by grouping the letters in a bigram. By using a 5x5 keyboard, we can encrypt plaintext (original text data to be encrypted) and decrypt the ciphertext (encrypted text data) by grouping it by removing the letter J from plaintext. The keypad is generated randomly by the software so that each encoding process (encryption and decryption) can use different keys. The software is also used to prove the correctness of the encryption and decryption results of the Playfair Cipher with cube keyboards. Cipher Playfair software is developed using the C++ language and is console-based in a Windows development environment.

1. INTRODUCTION

The use of computer technology as one of the applications of information technology has become a necessity, because many jobs can be completed quickly, accurately, and efficiently [1]. With the development of telecommunication techniques and data processing systems that are closely related to communication between computer users with each other computers that serve to transmit data so that security problems are one of the important aspects. Finally, people are developing ways to address data security issues that are essentially how to prevent unauthorized, unable to read or even damage data that is not directed at them [2].

In data communication, there is a method of securing data known as cryptography. Cryptography is one of the methods of data security that can be used to maintain data confidentiality, data authenticity, and authenticity of transmission [3]. This method aims to prevent confidential information sent through public telecommunications from being known or used by persons who are not interested or who are not entitled to receive it. Cryptographic methods that can be used to secure data are manifold. Each method has its own advantages and disadvantages. However, the problem in choosing a suitable cryptographic method is how to know and understand how the cryptographic method works [4], [5]. In the process of data communication, even if the data has been encrypted, it is possible that the data can be known by others. One such possibility is that the person intercepted the communication media used by the two people who were communicating

2. METHODS

In collecting the data required for research, the authors use the following methods:

1. FieldResearch Method
   The method is to directly obtain the data needed to make the data more accurate. In this case data retrieval using the following methods:
2. Observation (Observation)
   Make observations by searching for data and information from the internet in solving problems.
3. Interview
   Conduct a live interview with lecturers or friends on matters related to this final assignment.
4. Study Library
   Using this method, the authors obtained data by quoting from some reading material related to research. The cited can be data, information, theories or some opinions from books obtained from the library.

2.1 PlayFair Chiper Algorithm

The Playfair cipher algorithm is a cryptographic algorithm developed by english physicist Sir Charles Wheatstone (1802 - 1875). This algorithm is called Playfair in honor of wheatstone's friend Lyon Playfair who has helped him popularize the algorithm through his efforts in lobbying the British government to use it officially [6], [7]. This algorithm was used for tactical purposes by british soldiers during World War I. This algorithm was chosen because it was fairly fast enough to be used and did not require any special equipment [8], [9]. A common scenario of using Playfair algorithms is to protect important but not critical messages during the war. Therefore, if enemy cryptologists can solve the algorithm, the information they get is not information that is important to them. Playfair's algorithm is a cipherdigraphsalgorithm, which means that every encryption process is performed on every two letters. Suppose plaintext is "cryptology", then the encryption process is done against "kr ip to lo gi". The key to cryptography is the 25 letters of the alphabet arranged in a 5 x 5 table by removing the letter J from the alphabet. The letter J is considered the same as the letter I, because in English, the letter J has the smallest frequency of occurrence [10], [11]. Each elementabel contains letters that are different from each other. Examples can be seen in the following table.

Table 1. lock on playfiar chiper

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

Of the key boards mentioned above, the number of possible keys is
25!=15,511,210,043,330,985,984,000,000
Things to note in ciphers using playfair chiper methods such as messages to be encrypted are set in advance as follows:

1. All spaces and characters that are not alphabetical should be omitted from plaintext.
2. If there is a letter J on plaintext then replace the letter with the letter I.
3. The message to be encrypted is written in a pair of letters(bigram).
4. If there are the same letters in pairs of letters, then insert the letter X or Z in the center. The inserted letter should be the letter X because it is very unlikely that there is the same letter X in bigram,unlike the letter Z, for example in the word FUZZY.
5. If the number of letters in plaintext is odd then select an additional letter selected by the person encrypting and add it at the end of plaintext. Additional letters can be selected arbitrarily e.g. letters Z or X.
6. The key is entered in a 5 x 5 size table with no repeating letters allowed.

3. RESULT AND DISCUSSION

3.1 Encryption Process

Encryption is a process by which the original text data is converted into confidential text data. Before encrypting, the message to be encrypted(plaintext)is set first as follows:

1. All spaces and characters that are not alphabetical should be omitted from plaintext.
2. If there is a letter J on the palintext then replace the letter with the letter I.
3. The message to be encrypted is written in a pair of letters(bigram).
4. If there are the same letters in pairs of letters, then insert the letter X or Z in the center. The inserted letter should be the letter X because it is very unlikely that there is the same letter X in bigram,unlike the letter Z, for example in the word FUZZY.
5. If the number of letters in plaintext is odd then select an additional letter selected by the person encrypting and add it at the end of plaintext. Additional letters can be selected arbitrarily e.g. letters Z or X.
6. The key is entered in a 5 x 5 size table with no repeating letters allowed.

Sample Problem : Message= DATA ENCODING WITH MY NEW COMPUTER SUCCEEDED

Key= NIGHT

The encryption algorithms for each bigram are as follows:

1. If there are two letters in the same key line then each letter is replaced with a letter to the right.
2. If there are two letters in the same column then each letter is replaced with letters underneath.
1. If two letters are not in the same row or the same column, then the first letter is replaced with the letter at the intersection of the first letter row with the second letter column.
2. The second letter is replaced with a letter at the fourth corner point of the rectangle formed from the 3 letters used so far.

Message Completion= **PE NY AN DI AN DA TA DE NG AN KO MP UT BA RU KU BE RH AS IL**

Key

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

Encrypt PE to KH shown on the keypad below

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

Encrypt NY to OX shown on the key board below

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

Encrypt AN to LK shown on the key board below

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

Encrypt DI to IQ shown on the key board below

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

Encrypt AN to LK shown on the key board below

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

Encrypt DA to EM shown on the keypad below

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

Encrypt TA to RB shown on the key board below

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

Therefore, from the above experiments can be obtained the results of encryption as follows:

Ciphertext:

KH OX LK IQ LK EM RB EF OF LK NP CI QU KW CL SQ PR AG UE LR NM

3.2 Decryption process

The decryption process is very similar to the encryption process and easier to do. To decrypt, ciphertext is grouped first in a pair of letters (bigram) as at the time ofencryption. Then, apply a decryption algorithm that is the opposite of the encryption algorithm for each bigram. The decryption algorithm is as follows:

1. If there are two letters in the same key line then each letter is replaced with the letter to the left (in the expanded key).
2. If there are two letters in the same key column then each letter is replaced with a letter above 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 with the letter at the intersection of the first letter row with the second letter column.
4. The second letter is replaced with the letter at the intersection of the second letter line with the first letter column.

After applying the decryption algorithm to the ciphertext, letters can have meaning by increasing the space between possible words. If there are letters that are between the same two letters (not in place) then the letter can be omitted in order to be able to read the message that has been decrypted properly. Examples of ciphertext that have been grouped in letter pairs.

KH OX LK IQ LK EM RB LC HE AP NP CI VU KW CL SQ PR AG UE LR NM

Decrypt KH to PE shown on the key board below

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

The descriptor ox to NY is shown on the key board below

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

Decrypt LK to AN shown on the key board below

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

Decrypting IQ to DI is shown on the key board below

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

Decrypt LK to AN shown on the key board below

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

Decrypting EM to DA is shown on the key board below

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

Therefore, from the above experiments can be obtained plaintext results as follows:

Plaintext= **PE NY AN DI AN DA TA DE NG AN KO MP UT BA RU KU** BE RH AS **IL**

4. CONCLUSION

Based on the results of testing and analysis of Algortima Playfair Cipher,can be drawn some conclusions that Playfair Cipher with a key board in the form of bujuesangkar can encode the message so that only the rightful party can see the content of the message. Playfair Cipher using cube-shaped keyboards is a better solution than square keyboards in addressing security and text data confidentiality issues. Playfair Cipher can only be used to encrypt and decrypt data in the form of alphabetic text so that if there are characters other than the alphabet it will be ignored (not in the archive of encryption results or decrypted archives). Ignored characters can be avoided by writing them in alphabetic text

REFERENCE

[1] M. Narzillo, S. Abdurashid, N. Parakhat, and N. Nilufar, “Automatic speaker identification by

voice based on vector quantization method," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, 2019, doi: 10.35940/ijitee.J9523.0881019.

[2] A. Salmanogli and D. Gokcen, "Analysis of quantum radar cross-section by canonical quantization method (full quantum theory)," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3037364.

[3] A. Farisi, "Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 4, no. 2, 2018, doi: 10.35957/jatisi.v4i2.103.

[4] S. Retno and N. Hasdyna, "ANALISIS KINERJA ALGORITMA HONEY ENCRYPTION DAN ALGORITMA BLOWFISH PADA PROSES ENKRIPSI DAN DEKRIPSI," *TECHSI - J. Tek. Inform.*, vol. 10, no. 2, 2018, doi: 10.29103/techsi.v10i2.858.

[5] W. M. Rahmawati and F. Liantoni, "Penggunaan Arnold Cat Map Dan Beta Chaotic Map Pada Enkripsi Data Citra," *J. ELTIKOM*, vol. 2, no. 2, 2018, doi: 10.31961/eltikom.v2i2.85.

[6] Amalia, M. A. Budiman, and R. Sitepu, "File text security using Hybrid Cryptosystem with Playfair Cipher Algorithm and Knapsack Naccache-Stern Algorithm," in *Journal of Physics: Conference Series*, 2018, vol. 978, no. 1, doi: 10.1088/1742-6596/978/1/012114.

[7] A. Hariati, K. Hardiyanti, and W. E. Putri, "Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks," *Sinkron*, vol. 2, no. 2, 2018.

[8] D. Kurniawan, A. L. Hananto, and B. Priyatna, "Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android," *Int. J. Comput. Tech.* –, vol. 5, no. 1, 2018.

[9] M. Z. Siambaton and A. Muhazir, "Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks," *J. Ilmu Komput. dan Inform.*, vol. 02, no. April, 2018.

[10] M. Din, S. K. Pal, S. K. Muttoo, and S. Madan, "A hybrid computational intelligence-based technique for automatic cryptanalysis of playfair ciphers," *Def. Sci. J.*, vol. 70, no. 6, 2020, doi: 10.14429/DSJ.70.15749.

[11] R. M. Marzan, A. M. Sison, and R. P. Medina, "Randomness analysis on enhanced key security of Playfair cipher algorithm," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 4, 2019, doi: 10.30534/ijatcse/2019/34842019.