ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 02, Number : 01, April 2018 ISSN 2598-6341 (online)

MODIFIKASI ALGORITMA *PLAYFAIR CIPHER* DENGAN PENGURUTAN *ARRAY* PADA MATRIKS

Mhd. Zulfansyuri Siambaton[1], Abdullah Muhazir[2]
[1]*Universitas Islam Sumatera Utara,* [2]*Institut Teknologi Medan*
[1]*ambaton3985@gmail.com*
[2]*muhazir@gmail.com*

Abstrak

Metode *Playfair Cipher* merupakan salah satu metode kriptografi yang telah lama dikenal dan masih dipakai sampai sekarang. Namun para kriptanalis berusaha untuk memecahkan metode tersebut sehingga dirasa perlu untuk memodifikasi *Playfair Cipher* dengan tujuan untuk meningkatan kemampuan dari keamanan yang diberikan. Dengan mengubah ukuran matriks menjadi 6x6 dengan menambahkan karakter 0-9 dan melakukan pengurutan berdasarkan *array* dalam memasukkan kedalam matriks, diharapkan dapat lebih kuat dari pada playfair standard.

Kata kunci : Kriptografi, *Playfair* Cipher, modifikasi.

Abstract

Playfair Cipher method is one of cryptography method that has long been known and still used until now. But the cryptanalysts are trying to solve the method so it is necessary to modify the Playfair Cipher in order to increase the ability of the security provided. By changing the size of the matrix to 6x6 by adding characters from 0 to 9 and sorting by array into insertion into the matrix, it is expected to be stronger than the standard playfair.

1. Pendahuluan

Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia, meski begitu, aspek negatifnya juga banyak, seperti kejahatan kemputer yang mencakup pencurian data, penipuan, pemerasan, kompetisi dan banyak lainnya. Jatuhnya informasi penting kepada pihak lain yang tidak berhak akan merugikan bagi si pemilik informasi.

Kerahasiaan dan keamanan data merupakan salah satu aspek terpenting yang perlu diperhatikan terutama didalam era digital ini dimana semua perangkat komputer baik yang bersifat desktop maupun mobilebisa terhubung satu sama lain dalam dunia maya. Hal ini sering dimanfaatkan para hacker untuk menyusup kedalam device untuk melakukan *cybercrime* misalnya dengan berusahamencuri data ataupun merubah data atau pesan aslinya.

Untuk menjaga aspek keamanan data dan demi alasan keamanan dan mempertahankan kerahasiaan pesan atau data, maka munculah teknik – teknik penyandian pesan atau yang lebih dikenal dengan nama kriptografi. Pesan atau data akan di ubah menjadi kode – kode yang tidak memiliki makna dan tidak dipahami, sehingga bila ada pihak lain yang tidak berhak, maka mereka tidak akan mengetahui makna sebenarnya pesan tersebut.

Metode *Playfair Cipher* adalah salah satu metode kriptografi yang telah lama dikenal dan masih banyak dipakai dan dipelajari sampai saat ini. Metode *playfair cipher* menggunakan pembentukan matriks berdasarkan kunci yang diketahui. Untuk memperkuat kerahasiaan data yang menggunakan metode ini, maka akandilakukan penelitian dengan modifikasi terhadap playfair cipher standar agar menjadi lebih kuat dan aman sehingga dapat mencegah

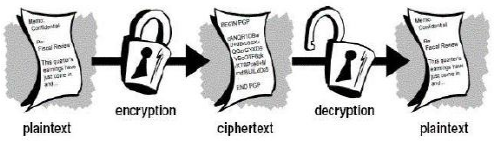
kriptanalis untuk memecahkan kriptografi sesuai dengan cara mereka memecahkan *playfair* cipher standar.

II. KAJIAN TEORI

1. Kriptografi

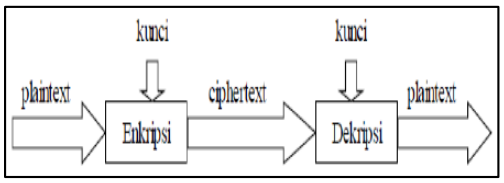
Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu *cryptos* dan *graphein*. *Cryptos* berarti rahasia, dan graphein berarti tulisan. Sehingga menurut bahasa, kriptologi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah suatu ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, integritas suatu data, serta otentifikasi data (Menezes,1996 : 4). Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plaintext) menjadi sebuah kode yang tidak bisa dimengerti (ciphertext).Sedangkan proses kebalikannya untuk mengubah ciphertext menjadi plaintext disebut dekripsi.

Menurut catatan sejarah, kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja – raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perang melalui kurir-kurirnya. Adapun diagram proses kriptografi pada mulanya dapat dilihat pada gambar berikut:



Gambar 1. Proses Kriptografi Pada Mulanya

Seiring perkembangan jaman dan teknologi, algoritma kriptografi pun mulai berubah ke arah algorima kriptografi yang lebih rumit dan kompleks. Algritma kriptografi pada awalnya merupakan permainan pergeseran alfabet saja, namun kemudian berkembang menjadi lebih kompleks misalnya diperlukannya *key* untuk melakukan enkripsi dan dekripsi.



Gambar 2. Mekanisme kriptografi

2. Playfair Cipher

Kode Playfair ditemukan oleh Sir Charles Wheatstone dan Baron Lyon. Kode Playfair pertama kali digunakan oleh tentara Inggris pada perang Boer (Perang Dunia I) pada tahun 1854 untuk mengirim pesan antar markas yang ada di Inggris.

Kunci dari *playfair cipher* adalah penggunaan matriks 5x5 (dengan masukan terdiri dari 25 karakter dengan membuat 1 karakter yang dianggap tidak digunakan atau jarang digunakan). Dengan begitu kunci yang digunakan ada 25 karakter. Jumlah kemungkinan dari kunci pada playfair cipher adalah 25! = 15.511.210.043.330.985.984.000.000.

Tabel 1. Matriks 5x5 Playfair

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

Sebelum melakukan enkripsi, maka harus dilakukan terlebih dahulu beberapa langkah berikut ini :

1. Tentukan metode matriks yang akan dipakai, apakah itu metode baris atau metode kolom.
2. Tentukan kunci dan jumlah pergeseran yang harus dilakukan. Misalnya jumlah pergeseran ditentukan ada 2.
3. Kunci yang diketahui harus di ekstrak terlebih dahulu agar tidak muncul huruf yang sama dalam tabel. Misalnya terdapat kata kunci INFORMATIKA. Maka di ekstrak menjadi INFORMATK.
4. Setelah kunci di ekstrak, masukan huruf-huruf kunci kedalam tabel, kemudian masukkan huruf-huruf dalam alfabet yang belum muncul ditabel secara berurutan. Huruf yang dihilangkan sesuai kesepakatan jangan dimasukkan kedalam tabel.

Tabel 2 : Matriks hasil ekstrak

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

5. Setelah terbentuk tabel kunci, maka plaintext dihilangkan dulu spasinya (bila ada) dan juga semua karakter yang bukan alfabet.
6. Pisahkan huruf-huruf pada plaintext menjadi pasangan huruf. Misalnya terdapat plaintext FULLMOON, maka dipisahkan menjadi FULLMOON.
7. Jika pada huruf terakhir tidak mendapatkan pasangan, maka ditambahkan huruf sendiri agar menjadi pasangan, misalnya tambahkan huruf X.
8. Jika ada huruf yang sama pada pasangan huruf (bigram), maka tambahkan huruf X ditengahnya dan bentuk kembali pasangan huruf yang baru. Misalnya FULLMOON dibentuk menjadi FULXLMOXON.

Untuk melakukan enkripsi dengan playfair cipher, ada beberapa langkah yang harus dilakukan, antara lain :

1. Jika 2 huruf dalam masing-masing pasangan huruf berada pada baris yang sama dalam tabel, maka huruf tersebut akan digeser sebanyak jumlah yang telah ditentukan per huruf ke arah kanan. Misalnya pada pasangan [ON]. Berdasarkan Tabel 1 huruf [ON] berada pada baris yang sama, maka untuk menentukan hasil enkripsinya dilakukan pergeseran sesuai yang ditentukan. Huruf O digeser sebanyak 2 kali. Karena pergeseran.
2. Mencapai ujung sebelum 2 kali, maka pergeseran kembali ke awal tabel. Sehingga dari pergeseran huruf O didapat huruf I. sedangkan pergeseran untuk huruf N didapatkan huruf O. sehingga untuk enkripsi huruf [ON] adalah [IO].
3. Jika 2 huruf dalam masing-masing pasangan huruf berada pada kolom yang sama dalam tabel, maka huruf tersebut akan digeser sebanyak jumlah yang telah ditentukan per huruf ke arah bawah. Misalnya pada pasangan [OX]. Berdasarkan Tabel 1 huruf [OX] berada pada kolom yang sama, maka untuk menentukan hasil enkripsinya dilakukan pergeseran sesuai yang ditentukan. Huruf O digeser sebanyak 2 kali. Sehingga dari pergeseran huruf O didapat huruf G. sedangkan pergeseran untuk huruf X didapatkan huruf K. sehingga untuk enkripsi huruf [OX] adalah [GK].
4. Jika pasangan huruf berada pada baris dan kolom yang berbeda, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Sedangkan untuk huruf kedua diganti dengan huruf pada perpotongan kolom huruf pertama dengan baris huruf kedua. Misalnya pada pasangan huruf [FU]. Maka berdasarkan tabel 2 didapat perpotongan di titik I, dan berdasarkan tabel 3 didapat perpotongan dititik W. sehingga enkripsi dari [FU] adalah [IW].

Tabel 3. Pencarian huruf pertama pada [FU]

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

Tabel 4. Pencarian huruf kedua pada [FU]

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

Berdasarkan cara enkripsi diatas, maka plaintext FULLMOON dapat dienkripsikan dengan playfair cipher, sehingga didapatkan hasil :

Plaintext : FULXLMOXON
Ciphertext : IW QV JA GK IO

Untuk melakukan dekripsi dengan playfair cipher, ada beberapa langkah yang harus dilakukan, antara lain :

1. Jika 2 huruf dalam masing-masing pasangan huruf berada pada baris yang sama dalam tabel, maka huruf tersebut akan digeser sebanyak jumlah yang telah ditentukan per huruf ke arah kiri.
2. Jika 2 huruf dalam masing-masing pasangan huruf berada pada kolom yang sama dalam tabel, maka huruf tersebut akan digeser sebanyak jumlah yang telah ditentukan per huruf ke arah atas.

3. Jika pasangan huruf berada pada baris dan kolom yang berbeda, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Sedangkan untuk huruf kedua diganti dengan huruf pada perpotongan kolom huruf pertama dengan baris huruf kedua.

Berdasarkan cara dekripsi diatas, maka ciphertext IWQVJAGKIO dapat dienkripsikan dengan playfair cipher, sehingga didapatkan hasil :

Ciphertext : IW QV JA GK IO
Plaintext : FU LX LM OX ON

III. PEMBAHASAN

Modifikasi Pada *Playfair* Cipher

Untuk modifikasi yang akan dilakukan, selain karakter alfabet (A-Z) yang diambil, maka karakter angka (0-9) juga akan digunakan sehingga matriks yang dibuat akan menjadi 6x6.

Pada fase pembentukan matriks, modifikasi akan dilakukan dengan langkah-langkah sebagai berikut:

1. Susun terlebih dahulu urutan alfabet dari A-Z kemudian dilanjutkan dengan 0-9. Keseluruhan karakter akan ditampung terlebih dahulu ke dalam range array dari 0-35.

Huruf	A	B	C	D	E	F	G	H	I
Array	0	1	2	3	4	5	6	7	8
Huruf	J	K	L	M	N	O	P	Q	R
Array	9	10	11	12	13	14	15	16	17
Huruf	S	T	U	V	W	X	Y	Z	0
Array	18	19	20	21	22	23	24	25	26
Huruf	1	2	3	4	5	6	7	8	9
Array	27	28	29	30	31	32	33	34	35

2. Kata kunciyang telah diketahui akan diekstrak terlebih dahulu sehingga tidak ada karakter yang double. Misalnya diketahui kata kunci INFORMATIKA, maka diekstrak menjadi INFORMATK.
3. Kata kunci yang telah diekstrak akan telebih dahulu dimasukkan kedalam matriks yang misalnya ditentukan adalah metode baris.

Tabel 5. Kata kunci yang dimasukkan ke matriks

I	N	F	O	M	A
T	K				

4. Indeks array yang menampung masing-masing karakter pada kata kunci akan di simpan terlebih dahulu. Kemudian karakter dari kata kunci akan dihapus dari array, kemudian membentuk urutan array baru dari karakter yang tersisa. Berdasarkan indeks array dari karakter pada kata kunci yang telah disimpan, akan diambil karakter yang tersisa berdasarkan indeks array yang di simpan ke dalam matriks.

Huruf	B	C	D	E	G	H	J	L	P
Array	0	1	2	3	4	5	6	7	8
Huruf	Q	S	U	V	W	X	Y	Z	0
Array	9	10	11	12	13	14	15	16	17
Huruf	1	2	3	4	5	6	7	8	9
Array	18	19	20	21	22	23	24	25	26

Tabel 6. Alfabet tersisa yang dimasukkan ke matriks

I	N	F	O	R	M
A	T	K	B	H	P
S	V	W	X	0	2

5. Dengan cara yang sama, bentuk kembali array baru berdasarkan karakter yang tersisa yang belum dimasukkan kedalam matriks. Berdasarkan indeks array yang tersimpan maka pilih lagi karakter yang akan dimasukkan ke dalam matriks.

Huruf	C	D	E	G	J	L	Q	U	Y
Array	0	1	2	3	4	5	6	7	8
Huruf	Z	1	3	4	5	6	7	8	9
Array	9	10	11	12	13	14	15	16	17

Tabel 7. Alfabet tersisa yang dimasukkan ke matriks

I	N	F	O	R	M
A	T	K	B	H	P

	S	V	W	X	0	2			
	C	L	Y	1	4	5			
	6	9							
Huruf	D	E	G	J	Q	U	Z	3	7
Array	0	1	2	3	4	5	6	7	8
Huruf	8								
Array	9								

Tabel 8. Alfabet tersisa yang dimasukkan ke matriks

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

Huruf	E	G	J	Q	Z	3	8
Array	0	1	2	3	4	5	6

Tabel 9. Alfabet tersisa yang dimasukkan ke matriks

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

Huruf	G	J	Q	Z	8
Array	0	1	2	3	4

Tabel 10 : Alfabet tersisa yang dimasukkan ke matriks

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

6. Setelah matriks terisi semua, maka proses untuk dekripsi dan enkripsi dilakukan dengan proses yang sama dengan playfair standar.

Berdasarkan cara enkripsi playfair standar, maka pada proses enkripsi jika terdapat plaintext FULLMOON akan dibentuk menjadi pasangan terlebih dahulu sehingga menjadi FULXLMOXON. Setelah itu dari pasangan huruf akan di proses kedalam matriks, sehingga hasil dari proses enkripsi adalah :

Plaintext : FULXLMOXON
Ciphertext : OD 1V 5N XU MO

Untuk proses dekripsi jika terdapat plaintext OD1V5NXUMO akan dibentuk menjadi pasangan terlebih dahulu sehingga menjadi OD1V5NXUMO. Setelah itu dari pasangan huruf akan di proses kedalam matriks, sehingga hasil dari proses dekripsi adalah :

Ciphertext : OD1V5NXUMO
Plaintext : FU LXLMOXON

IV. KESIMPULAN

Setelah dilakukan pembahasan dan percobaan terhadap perbandingan antara *playfair* standar dengan modifikasi dariplayfair, maka didapatkan bahwa dengan plaintext yang sama tetapi menghasilkan ciphertext yang berbeda. Hal ini dikarenakan tabel matriks *playfair* yang telahmengalami perubahan bentuk dimana matriks yang dibentuk adalah 6x6 dan huruf yang dimasukkan ke matriks menjadi acak sehingga menjadi susah untuk ditebak kombinasi yang beraturan dan kriptanalis tidak akan bisa memakai algoritma yang sama untuk membongkar algoritma modifikasi *playfair* cipher.

Modifikasi dari *playfair* cipher sebenarnya masih banyak bisa dilakukan untuk mendapatkan hasil matriks yang beda-beda ataupun ukuran matriks yang berbeda-beda sehingga kriptanalis tidak dapat menggunakan algoritma yang sama untuk membaca hasil enkripsi.

Daftar Pustaka

1. Choudhary J., Gupta R. K., Singh S., "A Generalized Version of Playfair Cipher", COMPUSOFT, An International Journal of Advanced Computer Technology, 2 (6), June 2013 (Voume-II, Issue-VI)
2. Shakil A. T., Islam R., "An Efficient Modification to Playfair Cipher", ULAB Journal of Science and Engineering, Vol. 5, No. 1, November 2014, ISSN: 2079-4398.
3. Alam A., Khalid S., Salam M., "A Modified Version of Playfair Cipher Using 7x4 Matrix", International Journal of Computer Theory and Engineering, Vol 5, No. 4, August 2013.
4. Choudhary J., Gupta R. K., Singh S., "A Survey of Existing Playfair Ciphers", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Volume-2, Issue-4, April 2013.
5. Bhattacharyya S., Chand N., Chakraborty S., "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue2, February 2014.
6. Ariyus, Donny. 2008. PENGANTAR ILMU KRIPTOGRAFI Teori, Analisis, dan Implementasi. Yogyakarta : Andi Offset.
7. Ariyus, Donny. 2005. Kriptografi: Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu