SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 1 Nomor 2, April 2017
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Analisis Matriks 5x7 Pada Kriptografi Playfair Cipher

Fadhillah Azmi
Universitas Sumatera Utara
Jl. Dr. Mansyur No 9 Medan
azmi.fadhillah007@gmail.com

Rina Anugrahwaty
Politeknik Negeri Medan
Jl. Alamameter No 1 Medan
rinaa_key@yahoo.com

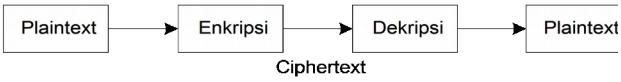
Abstrak **—** Kriptografi memiliki peran yang sangat penting di era digitalisasi yang mana bertujuan untuk mengamankan informasi. Informasi yang bersifat privasi dapat terhindar dari orang ketiga dan informasi yang akan disampaikan dapat dilindungi. Salah satu keamanan data yang ditawarkan dengan metode kriptografi *playfair cipher* yang mana sebelumnya telah dianalisa dengan menggunakan matriks 5x5, 7x4 dan 6x6. Tujuan dari penulisan ini untuk menganalisis matriks 5x7 pada metode kriptografi playfair cipher sejauh mana tingkat keamanan yang dapat diberikan dengan membandingkan hasil analisa yang telah dilakukan sebelumnya yaitu pada matriks 5x5, 7x4 dan 6x6.

Kata Kunci *— kriptografi, playfair, cipher, matriks.*

I. PENDAHULUAN

Secara etimologis, kriptografi berasal dari bahasa Yunani, yaitu crypto dan graphy. Crypto artinya secret dan graphy artinya menulis. Maka, kriptografi berdasarkan dari bahasanya didefinisikan sebagai menulis secara rahasia. [1].

Tujuan dari kriptografi adalah untuk membuat informasi baik berupa suara, teks, ataupun yang lainnya, dapat dilindungi privasi atau kerahasiannya pada saat dibagikan sehingga sampai ke tujuan yang dimaksud dalam satu saluran yang sama. Proses kriptografi terdiri dari enkripsi dan dekripsi. Di mana enkripsi adalah proses mengubah pesan asli (*plaintext*) menjadi pesan yang disandikan (*ciphertext*) berdasarkan metode yang telah ditentukan yang mana proses enkripsi bekerja dengan kunci untuk mengkonversi *plaintext* ke dalam *ciphertext*. Proses dekripsi adalah proses mengembalikan pesan yang disandikan (*ciphertext*) menjadi pesan asli (*plaintext*) sehingga informasi tersebut terjaga kerahasiaannya pada saat sampai ke tujuan yang mana proses dekripsi bekerja dalam urutan terbalik.



Gambar 1. Bentuk umum proses kriptografi

Ada dua proses pembentukkan kunci pada kriptografi, yaitu kunci simetris dan asimetris. Di mana kunci simetris memiliki kunci yang sama pada saat proses enkripsi dan dekripsi. Sedangkan, kunci asimetris memiliki kunci yang berbeda pada saat proses enkripsi dan dekripsi. Salah satu metode kriptografi yang memiliki kunci simetris adalah *playfair cipher*.[4].

Tujuan pembahasan ini adalah untuk mengetahui sejauh mana metode kriptografi ini dapat meningkatkan keamanan pada informasi yang mana pada penelitian sebelumnya telah dibahas dengan menggunakan matriks 5x5, 7x4 dan 16x16. Penulis menngunakan matriks 5x7 pada playfair cipher yang mana diharapkan lebih baik dari pada matriks sebelumnya.[5].

II. LANDASAN TEORI

A. Kriptografi

Secara etimologis, kriptografi berasal dari bahasa Yunani, yaitu *crypto* dan *graphy*. *Crypto* artinya *secret* dan *graphy* artinya menulis. Maka, kriptografi berdasarkan dari bahasanya didefinisikan sebagai menulis secara rahasia.

Kriptografi adalah sutau ilmu dan seni untuk mengamankan informasi yang berupa pesan yang terbaca (*plaintext*) menjadi pesan yang tidak bisa dibaca (*ciphertext*), sehingga hanya pengirim pesan dan penerima pesan yang dapat mengganti, menghapus dan membaca pesan tersebut. Ada dua proses pembentukkan kunci pada kriptografi, yaitu kunci simetris dan asimetris. Di mana kunci simetris memiliki kunci yang sama pada saat proses enkripsi dan dekripsi. Sedangkan, kunci

e-ISSN : 2541-2019
p-ISSN : 2541-044X

asimetris memiliki kunci yang berbeda pada saat proses enkripsi dan dekripsi. Salah satu metode kriptografi yang memiliki kunci simetris adalah *playfair cipher*.

Selain menyandikan pesan, kriptografi juga memiliki beberapa keamanan adalah sebagai berikut:[3].

1. *Confidentiality*, digunakan untuk menjaga pesan dari pihak yang tidak berhak terhadap pesan tersebut.
2. *Data integrity,* digunakan untuk menjamin pesan masih dalam bentuk asli/utuh atau tidak pernah dimodifikasi atau dimanipulasi selama pengiriman.
3. *Authentication*, digunakan untuk mengidentifikasi kebenran pihak-pihak yang berkomunikasi untuk mengidentifikasi kebenaran sumber pesan.
4. *Non-repudiantion,* digunakan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Proses kriptografi terdiri dari enkripsi dan dekripsi. Proses enkripsi adalah proses konversi *plaintext* ke dalam bentuk *ciphertext*, dan sebaliknya untuk proses dekripsi yang mana proses konversi *ciphertext* ke dalam bentuk *plaintext*. Parameter yang perlu dilakukan adalah pembentukkan kunci yang mana kunci tersebut digunakan untuk tranformasi proses enkripsi dan dekripsi.

B. Playfair Cipher

Playfair cipher atau sandi playfair ditemukan oleh Charles Wheatstone pada tahun 1854 yang mana dulu populer disebut *Lord Playfair*. Proses pembentukkan kunci pada metode ini hampir mirip dengan metode kriptografi *Vigenere Cipher*, tetapi pada *playfair cipher* memiliki teknik pemetaan yang lebih sulit jika dibandingkan dnegan *Vigenere Cipher*.[1].

Adapun tahapan enkripsi dalam pembentukkan kunci pada *playfair cipher* adalah sebagai berikut:[2].

1. Susun huruf ke dalam bentuk matriks $n \times n$ dengan menghilang huruf yang sama atau berulang dari abjad kunci, dan tambahkan huruf yang belum ada.
2. Koreksi apabila terdapat dua huruf yang sama pada baris kunci, maka tiap huruf diganti dengan huruf di kanannya.
3. Apabila terdapat dua haruf pada kolom kunci yang sama, maka huruf tersebut harus diganti dengan huruf di bawahnya.
4. Apabila pada baris atau kolom tidak terdapat dua huruf tidak yang sama, maka huruf pertama harus diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Selanjutnya, huruf kedua diganti dengan huruf pada titik sudut keempat dari matriks persegi tersebut yang dibentuk dari 3 huruf.

Selanjutnya untuk tahapan dekripsi untuk mengkonversi *ciphertext* ke dalam *plaintext* pada *playfair cipher* adalah sebagai berikut:

1. Apabila terdapat huruf J, maka diganti dengan huruf I.
2. Tulis pesan dalam pasangan huruf.
3. Tidak boleh terdapat huruf yang sama, tetapi jika terdapat huruf yang sama, maka sisipkan huruf Z di tengahnya.
4. Apabila terdapat jumlah huruf ganjil, maka tambahkan huruf Z di akhir dari matriks yang telah dibentuk.

III. PEMBAHASAN

Penulis melakukan pemabahasan kasus ini untuk untuk menganalisa matriks 5x7 yang mana diharapkan dapat memberikan tingkat keamanan yang lebih dari sebelumnya. Dalam kasus ini pembentukkan kunci dengan menggunakan matriksi persegi yaitu matriks 5 x 7.

Misalkan kunci yang dipilih adalah TEKNIK INFORMATIKA. Kemudian dilakukan proses enkripsi, adalah sebagi berikut:

1. Kunci yang dipilih TEKNIK INFORMATIKA, cek huruf yang sama dan apabila jika terdapat huruf J maka diganti dengan huruf I. Sehingga, diperoleh TEKNIFORMA dan tambahkan dengan huruf abjad untuk sisanya yang tidak terdapat pada kunci tadi.

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

2. Selanjutnya *plaintext* yang akan diamankan adalah KRIPTOGRAFI. *Plaintext* tersebut dibentuk berpasangan, yaitu :
   KR IP TO GR AF IZ

   KR:

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

   Dua huruf *plaintext* tersebut tidak satu baris tetapi satu kolom, maka huruf R turun 1 tingkat ke bawah menjadi D, dan K turun ke bawah menjadi huruf R,

e-ISSN : 2541-2019
p-ISSN : 2541-044X

karena R disebut pembanding K, sehingga *ciphertext* dari KR adalah RD.

IP:

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

Dua huruf *plaintext* tersebut tidak satu baris dan tidak satu kolom, maka huruf I turun 1 tingkat ke bawah menjadi A, dan P turun ke bawah menjadi huruf W, sehingga *ciphertxt* dari IP adalah TU.

TO:

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

Sama seperti *plaintext* sebelumnya, maka ciphertext dari TO adalah EF.

GR:

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

Sama seperti *plaintext* sebelumnya, maka ciphertext dari GR adalah DM.

AF:

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

Sama seperti *plaintext* sebelumnya, maka ciphertext dari AF adalah FO.

IZ:

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

Sama seperti *plaintext* sebelumnya, maka ciphertext dari IZ adalah TV.

Dari proses enkripsi di atas diperoleh *ciphertext* dari *plaintext* KR IP TO GR AF IZ adalah RD TU EF DM FO TV.

3. Untuk mengembalikan *ciphertext* ke bentuk *plaintext* dilakukan dengan proses dekripsi, adalah sebagai berikut:

RD:

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

Maka, *plaintext* dari RD adalah KR.

TU:

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

Maka, *plaintext* dari TU adalah IP.

EF:

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

Maka, *plaintext* dari EF adalah TO.

DM:

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

Maka, *plaintext* dari DM adalah GR.

FO:

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

Maka, *plaintext* dari FO adalah AF.

TV:

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

Maka, *plaintext* dari TV adalah IZ.

Dengan proses dekripsi dapat diperoleh kembali *plaintext* yang sesuai dengan aslinya, tetapi disini karakter huruf pada *plaintext* memiliki jumlah ganjil yang mana huruf Z ditambahkan pada akhir dari kalimat dapat langsung dihilangkan.

Dari pembahasan di atas, metode kriptografi dengan menggunakan playfair cipher yang mana matriks yang dipilih adalah 5 x 7, memiliki keterbatasan karakter yang mana karakter yang hanya digunakan yaitu huruf kapital dan angka saja, karakter lain seperti huruf kecil dan karakter lainnya tidak dapat dikonversi atau pun dipergunakan.

IV. KESIMPULAN

Berdasarkan dari pembahasan permasalahan kasus di atas dapat diambil kesimpulan:

1. Apabila jumlah pesan (*plaintext*) memiliki jumlah karakter ganjil, maka dapat ditambahkan karakter lain yang tidak sama pada akhir dari pesan.
2. Bentuk matriks yang dipilih mempengaruhi pesan yang akan diamankan, sehingga tidak semua karakter dapat diamankan, maka penulis menyarankan untuk memilih bentuk matriks yang lebih besar, misalnya sejumlah karakter pada *keyboard*.
3. Dengan mnggunakan matriks 5x7, tingkat keamanan yang dihasilkan ternyata tidak baik karena memiliki keterbatasan karakter yaitu huruf kapital dan numerik saja, sehingga konversi untuk data yang lain tidak dimungkinkan untuk diamankan.

REFERENSI

[1] Arora, Monika dan Sandiliya, Anish. 2015. *Design and Analysis of Modified Playfair Square Cipher Algorithm Using 6 by 6 Matrix with Five Iteration Steps and its Implementation in C/C++*. International Journal of Science and Research (IJSR),vol. 4, Issue 6 June 2015.

[2] Andriana, Egi. 2016. Algoritma Enkripsi Playfair Cipher. https://www.researchgate.net/publication/303374525.

[3] Bhowmick, Anirban., Lal, Vardhan., dan Ranjan, Nitish. 2015. *Enhanced 6x6 Plaufair Cipher Using Double Myszkowski Tranposition.* International Journal of Engineering Research&Technology (IJERT), vo. 4, Issue 07, July 2015.

[4] Bodkhe, Bhagyashree dan Jain Dc. 2012. *An Enhanced Playfair Cipher Cryptographic Subsitution Algorithm with 6x6 Matrix*. Journal of Current Engineering RFesearch, vol. 2, issue 3, May-June 2012.

[5] Dhenakaran, SS dan Ilayaraja, M. 2012. *Extension of Playfair Cipher Using 16x16 Matrix*. International Journal of Computer Applications, vol. 48, No. 7, June 2012.