MODIFIKASI TABEL CIPHER PADA ALGORITMA PLAYFAIR

E. Haodudin Nurkifli[1]
[1]Teknik Informatika, Ilmu Komputer, Universitas Singaperbangsa Karawang
Jl. H.S. Ronggo Waluyo / Teluk Jambe Karawang
[1]dudi.nurkifli@staff.unsika.ac.id

ABSTRAK

Playfair Cipher merupakan metoda enkripsi klasik yang sangat sulit untuk dikriptanalisis secara manual. Meskipun demikian *Playfair* dapat dipecahkan dengan menggunakan informasi frekuensi kemunculan bigram. Komponen yang penting pada algoritma playfair adalah tabel cipher yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5x5) yang berisi huruf kapital dari A- Z dengan menghilangkan J. Tabel bawaan yang ada pada playfair cipher tidak dapat mengenkripsi Plainteks yang berisi huruf kecil (a-z), angka (0-9) dan simbol-simbol. Kelemahan yang lain pada playfair adalah terjadinya ambigu pada hasil dekripsi karena pada persiapan enkripsi, playfair cipher memiliki mekanisme mengganti J dengan I. Modifikasi tabel playfair chiper yang dapat digunakan untuk melakukan enkripsi huruf kapital, huruf kecil, angka dan simbol. Penggunaan tabel 12 x 12 yang sangat acak memiliki Confusion yang bagus sehingga membuat hubungan statistik antara plainteks, cipherteks, dan kunci menjadi sangat rumit.

Kata Kunci: *Playfair, Tabel Cipher, Confusion, Diffusion*

PENDAHULUAN

Playfair Cipher merupakan metoda enkripsi klasik yang sangat sulit untuk dikriptanalisis secara manual. Meskipun demikian *Playfair* dapat dipecahkan dengan menggunakan informasi frekuensi kemunculan bigram. Komponen yang penting pada algoritma playfair adalah tabel cipher yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang berbentuk matrik berukuran (5x5) yang berisi huruf kapital dari A- Z dengan menghilangkan J.

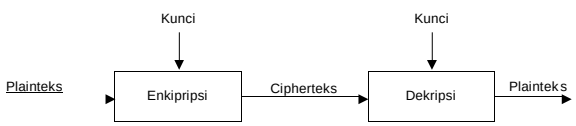
Ciphertek hasil enkripsi relatif mudah dipecahkan ketika kriptanalisis mengetahui cipherteks dan tabel ciphernya, walaupun kriptanalis hanya mengetahui cipherteks tanpa mengetahui tabel chiper kriptanalis dapat menebak bigram berdasakan huruf yang bermakna dari sebuah kata [1-9, 11].

Tabel bawaan yang ada pada playfair cipher tidak dapat mengenkripsi Plainteks yang berisi huruf kecil (a-z), angka (0-9) dan simbol-simbol. Kelemahan yang lain pada playfair adalah terjadinya ambigu pada hasil dekripsi karena pada persiapan enkripsi playfair cipher memiliki mekanisme mengganti J dengan I [3,5,6,8]. Perlunya modifikasi tabel playfair chiper yang dapat digunakan untuk melakukan enkripsi huruf kapital, huruf kecil, angka dan simbol. Mengacak isi tabel diperlukan agar cipherteks yang dihasilkan menjadi acak.

METODE PENELITIAN

Metode penelitian berdasarkan skema kriptografi disajikan pada gambar 1.

.



Gambar 1. Skema enkripsi dan dekripsi

Gambar 1 memperlihatkan beberapa hal yang akan dibahas: penentuan kunci, proses enkripsi dan proses dekripsi. penelitian ini menyajikan bagaimana melakukan proses modifikasi terhadap algoritma playfair.

Playfair Cipher menggunakan papan kunci yang berbentuk bujursangkar dalam melakukan penyandian. Papan kunci ini berukuran 5x5, dimana setiap bagian dalam papn kunci mewakili huruf-huruf dalam alfabet (abjad) dengan menghilangkan huruf J dari abjad. Setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain [10].

Tabel 1. Tabel cipher playfair (5x5)

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

Algoritma Persiapan Enkripsi *Playfair Cipher*

Sebelum melakukan enkripsi, pesan yang akan dienkripsi (plainteks) diatur terlebih dahulu sebagai berikut :

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari plainteks (jika ada).
2. Jika ada huruf `J` pada palinteks maka ganti huruf tersebut dengan huruf `I`.
3. Pesan yang akan dienkripsi ditulis dalam pasangan huruf (*bigram*).
4. Jika ada huruf yang sama dalam pasangan huruf, maka sisipkan huruf `X` atau `Z` di tengahnya. Huruf yang disisipkan sebaiknya huruf `X` karena sangat kecil kemungkinan terdapat huruf `X` yang sama dalam *bigram*, tidak seperti huruf `Z`, contohnya dalam kata `FUZZY`.
5. Jika jumlah huruf pada plainteks adalah ganjil maka pilih sebuah huruf tambahan yang dipilih oleh orang yang mengenkripsi dan tambahkan di akhir plainteks. Huruf tambahan dapat dipilih sembarang misalnya huruf `Z` atau `X`.

Algoritma Enkripsi *Playfair Cipher*

Algoritma enkripsi untuk setiap *bigram* adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan

Algoritma Dekripsi *Playfair Cipher*

Algoritma dekripsi merupakan kebalikan dari algoritma enkripsi untuk setiap *bigram* adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di atasnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan

Contoh enkripsi dan dekripsi

Plaintek: IT IS FULL MOON. Buat bigram dari Plainteks gantikan j dengan i, tambahkan X jika pasangan huruf ganjil. “IT IS FU LX LM OX ON”. Enkripsi dengan cara megnacu pada tabel cipher matrik 5x5 dengan isi tabel sembarang. Tabel acuan enkripsi table

Tabel 2. Tabel cipher playfair (5x5)

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

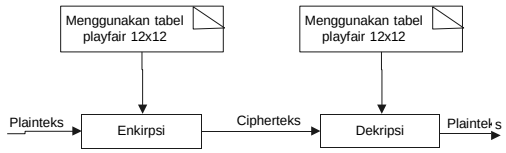
Cipherteks yang dihasilkan: DM GZ BZ PY KV TR MR Proses dekripsi merupakan kebalikan dari proses enkripsi. Cipherteks yang dihasilkan "DM GZ BZ PY KV TR MR" dilihat berdasarkan tabel DM sehingga pasangan bigram plaintek "IT". Hasil pasangan bigram menjadi "IT IS FU LX LM OX ON". Hilangkan X menjadi "IT IS FU L LM OON" palinteks "IT IS FULL MOON" [10].

HASIL DAN PEMBAHASAN

Hasil dan pembahasan menjelaskan usulan algoritma skema baru algoritma playfair, modifikasi matriks dari play fair dan kriptanalisis.

Usulan Skema Baru Algoritma Playfair

Beberapa hal yang harus dipersiapkan untuk melakukan proses enkripsi dan dekripsi yang mengacu pada stalling (2010).



Gambar 2. Skema enkripsi dan dekripsi playfair

Gambar 2 Memperlihatkan skema dari algoritma playfair. Enkripsi terhadap palinteks membutuhkan tabel playfair. Tabel playfair dimodifikasi sehingga menjadi tabel playfair 12x12. Modifikasi tabel disajikan pada subab 6. Plainteks di enkripsi menghasilkan cipherteks, Proses untuk mengembalikan dilakukan dengan mendekripsi cipherteks sehingga menjadi Plainteks.

Modifikasi Playfair Matriks (12x12)

Tabel yang dibentuk tidak berdasarkan kunci, tabel terdiri dari 12 baris dan 12 kolom berisi huruf kapital (A-Z), huruf kecil (a-z), angka (0-9) dan simbol. Tabel bentukan diperlihatkan pada tabel 3.

Tabel 3. Tabel cipher (12 x 12)

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
Z	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	z	0	1	2	3	4	5	6	7	8	9
#	$	%	^	&	*	(	)	-	=	+	[
]	;	„	:	“	\	,	.	/	<	>	?
£	¥	@	***β***	***π***	***σ***	***μ***	***τ***	∞	±	≥	≤
÷	À	Á	Â	Ä	È	É	Ê	Ë	Ì	Í	Î
Ï	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Ü
Ý	à	á	Â	ä	å	æ	ç	è	é	ê	Ë
ì	í	î	Ï	ð	ñ	ò	ó	ô	õ	ù	Ü

Proses enkripsi dan dekripsi sama halnya dengan playfair cipher biasa. Misalkan plaintek: "Temui aku di kampus jam 7 atau jam 9 pagi". Bigram yang terbentuk "Te mu ia ku di ka mp us ia m7 at au ia m9 pa gi" pada bigram ada huru j sehingga setiap j harus diganti dengan i. pembentukan bigram tidak tersisa huruf ganjil dan bigram tidak memiliki huruf sama sehingga tidak perlu menggantikan atau menambahkan dengan X.

Proses enkripsi mengacu pada tabel cipher sehingga cipherteksnya "Sf nv kb hw ek lb nq tv kb vy gn hn kb xy nc". Proses dekripsi akan menghasilkan bigram "Te mu ia ku di ka mp us ia m7

at au ia m9 pa gi". Terjadinya ambigu saat dekripsi dikarenakan ada mekanisme menggantikan j dengan i, misalkan jam menjadi iam.

Pembuktian penerapan playfair dengan kunci dan isi tabel tidak terlalu acak. Kunci: M@h@∞*15wa* buat tabel cipher berdasarkan kunci. Isikan tabel dengan huruf, angka, simbol yang belum ada mengacu pada isi tabel 3. Sehingga membentuk tabel 4

Tabel 4. Tabel cipher (12 x 12)

M	@	H	∞	1	5	W	a	A	B	C	D
E	F	G	H	I/J	K	L	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	b	c	d	e
f	g	i/j	k	l	M	n	o	p	q	r	s
t	u	V	x	y	Z	0	2	3	4	6	7
8	9	#	$	%	^	&	*	(	)	-	=
+	[	]	;	„	:	“	\	,	.	/	<
>	?	£	¥	***β***	***π***	***σ***	***μ***	***τ***	±	≥	≤
÷	À	Á	Â	Ä	È	É	Ê	Ë	Ì	Í	Î
Ï	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Ü
Ý	à	Á	â	ä	Å	Æ	ç	è	é	ê	ë
ì	í	Î	ï	ð	Ñ	Ò	ó	ô	õ	ù	ü

Enkripsi plaintek "Temui aku di kampus jam 7 atau jam 9 pagi". Buat bigram "Te mu ia ku di ka mp us ia m7 at au ia m9 pa gi" menghasilkan cipherteks " Us gz oh gx Ur o∞ nq 7g oh sz M2 @2 oh g^ oA ik ". Proses dekripsi bermula ditemukanya bigram "Te mu ia ku di ka mp us ia m7 at au ia m9 pa gi". Masih terjadi ambigu terhadap i yang mana yang akan dirubah menjadi j. tidak terlalu mengacak isi tabel sehingga penambahan angka dan simbol pada isi tabel tidak berpengaruh.

Pembuktian modifikasi tabel cipher yang disi secara acak Kunci: M@h@∞*15wa* buat tabel cipher berdasarkan kunci. Isikan tabel dengan huruf, angka, simbol yang belum ada mengacu pada isi tabel 3 cara pengisiannya dilakukan dengan cara acak. Sehingga membentuk tabel 5

Tabel 5. Tabel cipher (12 x 12)

M	@	h	∞	1	5	W	a	=	B	C	D
β	***π***	G	H	]	K	L	N	<	P	≥	R
S	T	3	4	[	X	*	Z	B	÷	Í	)
f	&	i/j	K	l	***τ***	\	o	P	Ï	r	.
t	“	v	X	y	Ë	0	2	F	W	6	7
8	9	#	$	%	^	g	Y	(	e	-	A
+	U	V	;	„	:	u	n	,	s	/	O
>	?	£	¥	I/J	E	***σ***	***μ***	M	±	Q	≤
c	À	Á	Â	Ä	È	É	Ê	Z	Ì	d	Î
q	Ð	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Ü
Ý	à	á	Â	ä	Å	Æ	ç	È	é	ê	ë
ì	í	î	Ï	ð	Ñ	Ò	ó	Ô	õ	ù	ü

Enkripsi plaintek "Temui aku di kampus jam 7 atau jam 9 pagi". Buat bigram "Te mu ia ku di ka mp us ia m7 at au ia m9 pa gi" menghasilkan cipherteks "÷9 ***σ***, oh \; Ar o∞ zF n/ oh ≤F M2 Wn oh ?(o= #\". Proses dekripsi bermula ditemukanya bigram "Te mu ia ku di ka mp us ia m7

at au ia m9 pa gi". Masih terjadi ambigu terhadap i yang mana yang akan dirubah menjadi j. Isi tabel yang sangat acak menghasilkan cipherteks yang sangat acak.

Pembuktian menghingkan ambigu saat proses dekripsi . Kunci: M@h@∞*15wa* buat tabel cipher berdasarkan kunci. Isikan tabel dengan huruf, angka, simbol yang belum ada mengacu pada isi tabel 3 cara pengisiannya dilakukan dengan cara acak. Sehingga membentuk tabel 6

Tabel 6. Tabel cipher (12 x 12)

M	@	h	∞	1	5	W	a	=	B	C	D
β	π	G	H	]	K	L	N	<	P	≥	R
S	T	3	4	[	X	*	Z	B	÷	Í	)
f	&	j	K	l	τ	\	o	P	Ï	r	.
t	“	v	X	y	Ë	0	2	F	W	6	7
8	9	#	$	%	^	g	Y	(	e	-	A
+	U	V	;	„	:	u	n	,	s	/	O
>	?	£	¥	J	E	σ	μ	M	±	Q	I
c	À	Á	I	Ä	È	≤	Ê	Z	Ì	d	Î
q	Đ	Ñ	Ò	Ó	Ô	Õ	Ö	Ø	Ù	Ú	Ü
Ý	à	á	Â	ä	å	Æ	ç	È	é	ê	ë
ì	í	î	Ï	ð	ñ	Ò	ó	Ô	õ	ù	ü

Enkripsi plaintek “Temui aku di kampus jam 7 atau jam 9 pagi”. Buat bigram “Te mu ia ku di ka mp us ja m7 at au ja m9 pa gi” menghasilkan cipherteks “÷9 σ, Ë∞ \; Ar o∞ zF n/ oh ≤F M2 Wn oh ?(o= #\”. Proses dekripsi bermula ditemukanya bigram “Te mu ia ku di ka mp us ja m7 at au ja m9 pa gi”. Isi tabel yang lengkap dapat menghilangkan ambigu dalam proses dekripsi. tabel yang acak akan menghasilkan cipher yang acak.

Kriptanalisis

Confusion kriptografi merupakan hasl yang sangat penting. Confusion merupakan prinsip yang menyembunyikan hubungan apapun yang ada antara plainteks, cipherteks, dan kunci. Prinsip confusion akan membuat kriptanalis sukar untuk mencari pola-pola statistik yang muncul pada cipherteks. Penggunaan tabel 12 x 12 yang acak memiliki Confusion yang bagus sehingga membuat hubungan statistik antara plainteks, cipherteks, dan kunci menjadi sangat rumit.

KESIMPULAN

Berdasarkan analisis kriptanalis ada beberapa kesimpulan sebagai berikut:

a. Tabel cipher pada algoritma playfair menjadi komponen penting untuk enkripsi dan dekripsi
b. Tabel cipher dapat dimodifikasi menjadi ukuran tabel sembarang minimal menampung huruf kapital (A-Z).
c. Isi tabel dapat di isi dengan huruf-huruf dan simbol yang diisikan secara acak sehingga dapat memperkuat cipherteks

DAFTAR PUSTAKA

Aftab, A. A., Shah, B. K., dan Muhammad, C. S., A Modified Version of Playfair Cipher Using 7×4 Matrix., International Journal of Computer Theory and Engineering., Volume 5., No. 4., Agustus., 2013

Choudhary, J., Kumar, R. G dan Singh, S., A Generalized Version of Play Fair Cipher., international journal of advanced computer technology., Volume 2., PP 2-6, Juni., 2013

Harris, J., dan Attia, A., Modified Version of Cryptography Playfair Cipher with 8x8 Linear Feedback Shift Register., European Journal of Industrial and System Engineering., Volume 11., 2013

Kumar, D. M., dan Jain, D., The Problem Analysis on Encryption Technique in Cryptography., International Journal of Societal Applications of Computer Science., Volume 2., Mei., 2013

Kumar, V., et al., Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept., International Journal of Innovative Technology and Exploring Engineering., Volume 3., Juni., 2013

Nidhal, O. A. H., dan Wasfi, B. A., 11 × 11 Playfair Cipher based on a Cascade of LFSRs., IOSR Journal of Computer Engineering., Volume 12., PP 29-35., Mei-Juni., 2013

Ravindra, K. B., Udaya, S. K., dan Vina, A. B., A Survey on Recently Modernized Cryptographic Algorithms and Analysis on The Block Cipher Generation Using Play Color Cipher Algorithm., International Journal of Mathematical., Volume 2., November., 2011

Shakti, S. S., dan Gupta, N., A Novel Approach to Security using Extended Playfair Cipher., International Journal of Computer Applications., Volume 20.,c No.6., April., 2011

Shrivastava, G., Chouhan, M., dan Dhawan, M., A Modified Version Of Extended Plafair Cipher (8x8)., International Journal Of Engineering And Computer Science., Volume 2., No. 956 - 961., April., 2013

Stallings, W., Cryptography and Network Security: Principles and Practice., 5thedition, Prentice Hall., January 24., 2010.

Vatsa, S., Mohan, T., dan Vatsa, A. K., Novel Cipher Technique Using Subtitution Method., International Journal of Information and Network Security., Volume 1., No.4., PP 313-320., Oktober., 2012