ANALISIS *CRYPTANALYS EXHAUSTIVE SEARCH* DAN *STATISTICAL ATTACK* PADA ALGORITMA *PLAYFAIR CIPHER*

E.Haodudin Nurkifli[1], Deden Wahidin[2]

[1,2] Informatika, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang
[1] dudi.nurkifli@staff.unsika.ac.id, [2] deden.wahiddin@staff.unsika.ac.id

Abstrak

Kriptologi merupakan ilmu yang menekuni dua bidang yaitu kriptografi dan kriptanalisis. Kriptografi merupakan seni untuk mengacak sebuah pesan dengan teorema tertentu sehingga pesan tidak bisa dimengerti maknanya atau disebut dengan cipherteks. Kriptanalisis merupakan seni untuk memecahkan cipherteks tanpa mengetahui kunci yang digunakan. Ada banyak algoritma dalam kriptografi ataupun kriptanalisis Kajian penelitian ini memecahkan cipherteks yang dihasilkan oleh algoritma playfair dengan exhaustive key search dan statistical attack. Mekanisme pemecahan dengan exhaustive dilakukan dengan cara cryptanalis mengetahui algoritma yang digunakan dan mencoba pemecahan dengan segala kemungkinan kunci. Statistical attack memecahkan dengan cara mencari nilai frekuensi kemungkinan kata yang digunakan.

Kata kunci: Exhaustive Key Search, Stastical Attack

1. Pendahuluan

Kriptologi merupakan ilmu yang menekuni dua bidang yaitu kriptografi dan kriptanalisis. Kriptografi merupakan seni untuk mengacak sebuah pesan dengan teorema tertentu sehingga pesan tidak bisa dimengerti maknanya atau disebut dengan cipherteks. Kriptanalisis merupakan seni untuk memecahkan cipherteks tanpa mengetahui kunci yang digunakan. Ada banyak algoritma dalam kriptografi ataupun kriptanalisis.

Algoritma exhaustive key search merupakan algoritma untuk memecahkan cipherteks dengan cara mencoba satu persatu dengan kemungkinan kunci. Algortima playfair merupakan algoritma kriptografi yang memiliki pra-prosesing sebelum melakukan enkripsi dan enkripsi dilakukan terhadap tabel playfair. Algoritma statistical attack merupakan pemecahan cipherteks dianalisis berdasarkan kemunculan huruf.

Algoritma kriptografi yang handal merupakan algoritma yang sangat sukar dipecahkan atau untuk memecahkan cipherteks memerlukan waktu lama. Sebagian penelitian menggunakan kriptanalisis untuk mengukur kehandalan cipherteks yang dihasilkan oleh algoritma tertentu.

Penelitian ini akan membahasa bagaimana algoritma playfair bekerja menghasilkan cipherteks. Algoritma exhaustive key search dan statistical attack memecahkan cipherteks yang dihasilkan oleh playfair.

2. Tinjauan Pustaka

Aftab (2013), Chaoudhary (2013) memodifikasi tabel cipher menjadi 7x4 dan menambahkan dua simbol yaitu * dan #. menampilkan semua huruf (A-Z) Agar tidak terjadi ambigu saat melakukan dekripsi. semakin meningkatnya confusion dan diffusion akan mempersulit kriptanalis memecahkan cipherteks.

Harris dan Attia (2013), Shakti dan Gupta (2013) Memodifikasi ukuran tabel cipher menjadi 8x8 yang berisi huruf kapital (A-Z), angka (0-9) dan simbol. Selain memodifikasi tabel proses enkripsi digabungkan dengan algortima Linear Feedback Shift Register (LFSR). Ujicoba dengan cipherteks only attack, known Plainteks attack dan cipherteks attack tidak dapat memecahkan cipherteks dari playfair modifikasi. kekuatan tidak hanya substitusi dari matrik 8x8 akan tetapi karena digabungkan dengan cara mengacak bit menggunakan LFSR.

Khumar (2013) Memodifikasi tabel cipher menjadi 6x6 yang berisi (A-Z) dan (0-9). Menggabungkan pengacakan bit dengan LFSR setelah bit teracak baru melakukan enkripsi dengan playfair cipher tabel 6x6. Menggabungkan LFSR dan Playfair tabel cipher 6x6 dapat meningkatkan keamanan dari cipherteksnya.

Vatsa (2012) Memodeifikasi proses enkripsi pada Caesar cipher dengan membuat tabel up (4x4) dan tabel down (4x4). Menghindari brute force attack karena dengan tabel yang dibuat setiap huruf yang sama ketika dienkripsi tidak menghasilkan

huruf ciperteks yang sama. Pembentukan cipher dengan tabel dapat memperkuat cipherteks dari Caesar cipher.

Khumar (2013), Ravindra (2011) Membahasa beberapa kelemahan algoritma klasik: Caesar, playfair, vigenere, cipher hill. Kelemahan playfair cipher mudah ditebak jika kriptanalisis menemukan cipher dan kuncinya. Jika kriptanalisis hanya menemukan chiperteks maka kriptanalisis dapat menebak digram yang terbentuk dari cipherteksnya. Playfair dengan tabel cipher 5x5 tanpa modifikasi akan membuat cipher mudah dipecahkan.

Menurut Nidhal (2013) Pembuatan tabel playfair baru dengan ukuran 11x11 yang berisi (A-Z), (a-z), (0-9), beberapa simbol aritmatik. Lebih mengamankan di kombinisai dengan LFSR. Semakin meningkatnya confusion dan diffusion akan mempersulit kriptanalis memecahkan cipherteks.

Shrivastava (2013) Memodifikasi ukuran tabel cipher menjadi (8x8) dan menggunakan multi round untuk mengacak isi tabel cipher. Mempersulit pemechana analisis digram dan frekuensi analisis karena semakin acak isi tabel akan menghasilkan cipherteks yang acak.

3. Metodolgi

.

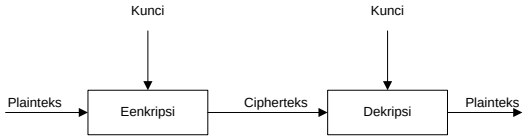
Metode yang digunakan dalama penelitian ini Hiatorical Reseach dengan tahapan :

a. Studi pustaka
   Tahap melakukan beberapa kajian kepustakaan mengenai algoritma playfair, algoritma exhaustive key search dan statistical attack menggunakan beberapa karyailmiah: Tesis, Desertasi, Jurnal nasional, jurnal internasional.
b. Analisis
   Tahap analisis melakukan kajian lebih mendalam terkait bagaimana algoritma playfair cipher bekerja mulai dari pra prosesing, pembentukan tabel kunci, proses enkripsi dan proses dekripsi. algoritma exhaustive key search melakukan penebakan plainteks dengan asumsi bahwa mengetahui algoritma yang digunakan untuk proses enkripsi dan dekripsi. algoritma statistical attack bagaimana memecahkan cipherteks dengan cara mengukur frekuensi kemunculan huruf.
c. Pengujian
   Tahap pengujian yaitu menguji algoritma exhaustive search key dan statistical attack dalam memecahkan cipherteks yang dihasilkan oleh algoritma playfair

4. Hasil dan Pembahasan

4.1 Algoritma Playfair

Ada dua proses dalam kriptografi yaitu enkripsi dan dekripsi. Enkripsi merupakan proses merubah plainteks menjadi cipherteks. Dekripsi merupakan proses pengembalian cipherteks menjadi plainteks. Skema enkripsi dan dekripsi tersaji pada gambar



Algoritma Playfair Termasuk ke dalam *polygram cipher* (salah satu tipe dari cipher substitusi). Ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tahun 1854. Playfair Cipher digunakan oleh tentara Inggris pada Perang Boer (Perang Dunia I).

Algoritma playfair memiliki tiga mekanisme: pembentukan bigram, enkripsi dan dekripsi.

Mekanime pemebentukan bigram:

1. Ganti huruf J (bila ada) dengan huruf. I
2. Tulis pesan dalam pasangan huruf (bigram).
3. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z di tengahnya
4. Jika jumlah huruf ganjil,tambahkan huruf Z di akhir

Proses enkripsi:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang sudah diperluas).
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas)
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. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Proses dekripsi:

4. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya (pada kunci yang sudah diperluas).
5. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di atasnya (pada kunci yang sudah diperluas)
6. 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. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Plainteks: AKU SEDANG BERNYANYI LAGU MERDU

kata kunci: RONGGO WALUYO

proses pembuatan bigram: AK US ED AN GB ER NY AN YI LA GU ME RD UZ
Pembentukan table kucni dari kata kunci terseji pada table

Tabel. Table kunci playfair

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

Proses enkripsi: IL AV EF UR YW CN GU RU AP UL NY VM OC BV

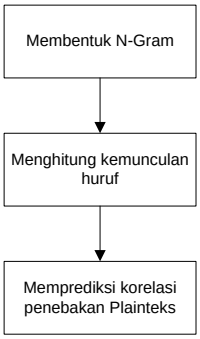
4.2 Exhaustive Key Search
Exhaustive Key Search merupakan algoritma untuk pemecahan cipherteks dengan cara mencoba satu persatu kunci.
Diketehui cipherteks: VHGDQJ. Pemecahan cipherteks dengan menggunakan algoritma exhaustive key search tersaji pada table.

Tabel Exhaustive Key Search mememecahkan cipherteks

Percobaan Ke-i	**Tebakan Plainteks**					
	V	H	G	D	Q	J
25	W	I	H	E	R	K
24	X	J	I	F	S	L
23	Y	K	J	G	T	M
22	Z	L	K	H	U	N
21	A	M	L	I	V	O
20	B	N	M	J	W	P
19	C	O	N	K	X	Q
18	D	P	O	L	Y	R
17	E	Q	P	M	Z	S
16	F	R	Q	N	A	T
15	G	S	R	O	B	U
14	H	T	S	P	C	V
13	I	U	T	Q	D	W
12	J	V	U	R	E	X
11	K	W	V	S	F	Y
10	L	X	W	T	G	Z
9	M	Y	X	U	H	A
8	N	Z	Y	V	I	B
7	O	A	Z	W	J	C
6	P	B	A	X	K	D
5	Q	C	B	Y	L	E
4	R	D	C	Z	M	F
3	S	E	D	A	N	G
2	T	F	E	B	O	H
1	U	G	F	C	P	I

Tabel di atas menyajikan kemungkinan besar plainteks yang dihasilkan adalah SEDANG, karena dari 25 kali pergeseran huruf pada pergeseran 3 merupakan kata yang bermakna.

4.3 Statistical Attack
Statistical attack merupakan pemecahan cipherteks dengan beberapa mekanisme tersaji pada gambar.



Gambar Skema Statistical Attack

Diberikan cipherteks: VHGDQJ
Step 1: Bentuk N Gram dari masing-masing karakter pada cipherteks. N Gram sebagai berikut: V H G D Q J
Step 2: Menghitung Frekuensi kemunculan huruf: Cipherteks memiliki 6 karakter yang terdiri 1 * {V, H, G, D, Q, J}. Buatlah fungsi terhadap cipherteks f(c): f(V) = 0.1, f(H)=0.1, f((G)=0.1, f(Q)=0.1, f(J)=0.1.
Step 3: menghitung korelasi dari masing-masing huruf dalam cipherteks terhadap kunci(k_i), untuk kunci *i*: $\varphi(i) = \Sigma_0 <= c <= 25\ f(c) * p(c - i)\ c$
C: V=21, H=7, G=6, D=3, Q16, J=9.
$\varphi(i) = 0.1p(21 - i) + 0.1p(7 - i) + 0.1p(6 - i) + 0.1p(3 - i) + 0.1p(16 - i) + 0.1p(9 - i)$

Tabel. Tabel korelasi frekuensi

i	**φ(i)**	**i**	**φ(i)**	**i**	**φ(i)**	**i**	**φ(i)**	**i**	**φ(i)**
0	6.2	6	2.6	12	-1	18	-4.6	24	-8.2
1	5.6	7	2	13	-1.6	19	-5.2	25	-8.8
2	5	8	1.4	14	-2.2	20	-5.8		
3	4.4	9	0.8	15	-2.8	21	-6.4		
4	3.8	10	0.2	16	-3.4	22	-7		
5	3.2	11	-0.4	17	-4	23	-7.6		

i=25, φ(i)=-8.8 dengan plainteks: WIHERK
i=24, φ(i)=-8.2 dengan palitneks: XJIFSL
i=3, φ(i)=4.4 dengan plainteks: SEDANG

5. Kesimpulan

1. Playfair melakukan enkripsi dan dekripsi menggunakan tabel kunci.
2. Statistical attack dan Exhaustive key Search tidak dapat memecahkan cipherteks yang dihasilkan oleh playfair dengan asumsi bahwa cryptSanalys tidak mengatahui algoritma yang digunakan untuk enkripsi

6. Saran

1. Perlu menggunakan algoritma lain untuk memecahkan playfair
2. Kriptanalis harus mengetahui algoritma yang digunakan untuk memecahkan cipherteks.
3. Mengkaji algoritma kasiski dalam pemecahan cipherteks yang dihasilkan oleh algoritma playfair.

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