H-Playfair Cipher

Hasanul Hakim / NIM : 13504091 [1)]
1) Program Studi Teknik Informatika ITB, Bandung,
email: if14091@students.if.itb.ac.id, haha_3030@yahoo.com

Abstract *– Playfair Cipher memiliki banyak kelemahan. Playfair Cipher dapat diserang dengan menggunakan teknik frekuensi distribusi huruf ganda pada suatu bahasa. Selain itu, Playfair Cipher tidak menyertakan huruf J sehingga bisa menimbulkan ambiguitas pada saat dekripsi.*
H-Playfair Cipher termasuk kedalam polygram cipher, salah satu tipe dari cipher subtitusi. H-Playfair Cipher adalah algoritma kriptografi yang mampu mengatasi kelemahan algoritma playfair biasa. H-Playfair Cipher menambah langkah algoritma Playfair biasa ditambah kunci diperluas menjadi bujursangkar 6x6. Tambahan langkah memiliki kemiripan dengan varian vigenere, tetapi fungsi penambahannya berbeda.
Makalah ini membahas tentang algoritma H-Playfair, keamanan H-Playfair, kekuatan dan kelemahan H-Playfair, serta kriptanalisis terhadap H-Playfair. Kriptanalisis yang dilakukan meliputi exhaustive attack, metode exhaustive key search, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, adaptive-chosen-plaintext attack, chosen-ciphertext attack, dan teknik analisis frekuensi.

Kata Kunci*: H-Playfair cipher, playfair cipher, polygram cipher, kriptanalisis, kriptografi.*

1. PENDAHULUAN

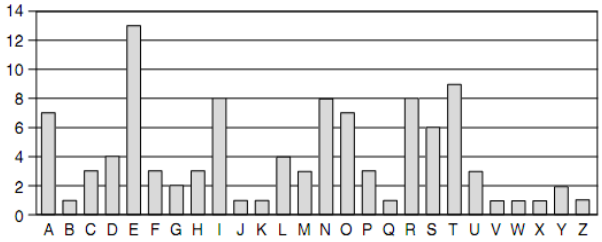
Playfair cipher adalah cipher klasik yang ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair[1]. Kekuatan dari algoritma ini adalah pada kuncinya yang menyusun bujursangkar 5x5. Kemungkinan kunci : 25! = 15.511.210.043.330.985.984.000.000.

Namun, playfair cipher bisa dipecahkan dengan teknik frekuensi distribusi ganda yaitu teknik yang menghitung frekuensi kemunculan pasangan dua huruf cipherteks yang kemudian dibandingkan dengan frekuensi pasangan dua huruf pada suatu bahasa. Disamping itu, hasil dekripsi playfair dapat menimbulkan ambiguitas karena saat enkripsi plainteks, semua huruf J pada plainteks diganti terlebih dahulu dengan huruf I.

Serangan-serangan yang mungkin dihadapi terhadap algoritma kriptografi H-Playfair antara lain:

1. *Exhaustive attack*
2. *Ciphertext-only attack*
3. *Known-plaintext attack*
4. *Chosen-plaintext attack*
5. *Adaptive-chosen-plaintext attack*
6. *Chosen-ciphertext attack*
7. Teknik analisis frekuensi

Teknik analisis frekuensi adalah teknik yang membandingkan distribusi kemunculan huruf pada *ciphertext* terhadap distribusi kemunculan huruf pada berbagai teks suatu bahasa. Lanjutannya adalah teknik analisis frekuensi pasangan huruf. Teknik analisis frekuensi pasangan huruf membandingkan distribusi dua huruf.



Gambar 1 : frekuensi distribusi huruf bahasa inggris[2]

Frekuensi kemunculan pasangan huruf dalam bahasa inggris dapat didekati dengan penghitungan pengalikan distribusi kemunculan sebuah huruf dengan distribusi huruf pasangannya. Jadi jika melihat pada gambar 1, frekuensi kemunculan pasangan huruf tertinggi adalah pasangan huruf ‘t’ dan ‘e’.

Algoritma kriptografi H-Playfair dikatakan aman apabila memenuhi kriteria berikut[1] :

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.
2. Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.
3. Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

2. ALGORITMA H-PLAYFAIR

H-Playfair termasuk kedalam polygram cipher sehingga H-Playfair dikategorikan juga algoritma kriptografi klasik. H-Playfair diciptakan sebagai

varian dari algoritma kriptografi playfair untuk mengatasi kelemahan playfair.

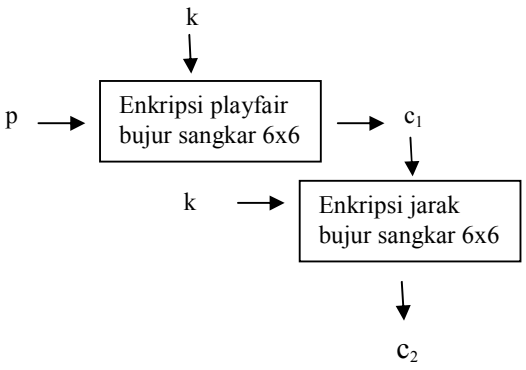
Kunci H-Playfair adalah 26 huruf (a,b,c,d,…,z) ditambah 10 buah angka (0,1,2,3,...,9) yang disusun di dalam bujur sangkar 6x6. Setiap bujur sangkar berisi huruf yang berbeda satu sama lain.

Contoh kunci :

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

Gambar 2: kunci H-Playfair

Algoritma enkripsi H-Playfair terdiri dari dua tahap. Yang pertama melakukan algoritma enkripsi sama dengan algoritma enkripsi playfair. Hanya saja bujursangkar berukuran 6x6 dan huruf j tetap ada. Tahap ke-dua melakukan algoritma lanjutan yang memiliki kemiripan dengan varian algorima kriptografi vigenere dengan fungsi substitusi berdasarkan jarak antar huruf di dalam bujursangkar 6x6.



Gambar 3: skema enkripsi H-Playfair

Algoritma enkripsi H-Playfair adalah sebagai berikut :

1) Pesan yang akan dienkripsi dituliskan dalam pasangan huruf. Jika dalam pasangan terdapat huruf yang sama, sisipkan huruf-huruf *dummy*. Jika terdapat huruf yang belum berpasangan, maka pasangkan huruf tersebut dengan *dummy*.

   Contoh plainteks:
   `saya hebat doong.`

   Dummy: DMY, plainteks menjadi :

   `sa ya he ba td od my on gd my`

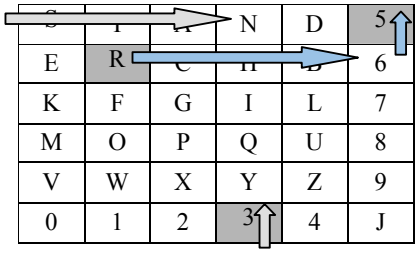
2) Lakukan algoritma seperti algoritma enkripsi playfair untuk mensubstitusikan semua pasangan huruf plainteks dengan bujursangkar kunci 6x6.

   Hasilnya menjadi :
   `tn xn br cd a5 ut qv qt la qv`

3) Hasil enkripsi tadi kemudian dikenakan algoritma enkripsi lanjutan. Huruf hasil enkripsi tadi dipasangkan dengan huruf pertama kunci untuk digantikan menjadi huruf baru menggunakan fungsi enkripsi jarak. Fungsi enkripsi jarak ini adalah menghitung jarak antara huruf yang akan dienkripsi dengan huruf kunci lalu mencari huruf dengan jarak yang sama terhadap kunci.
   Jika panjang kunci telah habis, sisanya diganti dengan huruf-huruf yang akan dienkripsi dari awal.

   contoh :
   plainteks: `tn xn br cd`
   kunci: `st an d5 er` (dari kotak 6x6)
   hasil: `55 gn 43 0l`

   Untuk huruf r dengan kunci 5 menghasilkan karakter 3. Jarak karakter 5 dari karakter r pada kotak adalah 4 petak kanan dan satu petak atas. Sehingga karakter dengan 4 petak kanan dan 1 petak atas dari karakter 5 (kunci) adalah 3 (jika melewati batas atas dan kanan maka definisi satu petak atas adalah karakter paling bawah pada kotak 6x6 pada kolom yang sama dan karakter paling kiri pada kotak 6x6 pada baris yang sama).



Gambar 4 : karakter r dan kunci 5 menghasilkan 3

Algoritma dekripsi kebalikan dari enkripsi yakni :

1) Cari karakter-karakter yang berjarak dari karakter kunci sama dengan karakter kunci ke cipherteks.
2) Lalu lakukan algoritma dekripsi playfair
3) Hilangkan dummy.

3. KRIPTANALISIS

3.1. Kekuatan algoritma kriptografi H-Playfair

Meskipun H-Playfair termasuk algoritma kriptografi klasik, tetapi kemampuan H-Playfair setara dengan kemampuan algoritma kriptografi modern yang memiliki prinsip membingungkan (*confusion)* dan menyebar (*diffusion)* [1].

Prinsip Shannon yang dipenuhi H-Playfair:

1) Confusion
   H-Playfair menyembunyikan hubungan antara cipherteks dan plainteks. Tidak seperti *caesar cipher* yang setiap huruf yang sama diganti menjadi huruf yang sama pula. Begitu pula dengan algoritma kriptografi playfair, yang setiap dua huruf yang sama diganti menjadi dua huruf yang sama pula.

   Prinsip *confusion* dapat terpenuhi karena pada H-Playfair dilakukan enkripsi dua tahap, kedua tahap saling berbeda.

   Tahap pertama seperti tahapan enkripsi playfair yang masih bisa dipecahkan dengan teknik frekuensi kemunculan pasangan huruf.

   Tahap kedua mirip seperti varian vigenere tanpa kunci yang diulang-ulang untuk substitusi, tetapi penambahan huruf kunci dengan huruf plainteks ke-dua (hasil enkripsi tahap pertama H-Playfair) bergantung pada posisi huruf-huruf pada kotak kunci 6x6. Tahap ke-dua tidak bisa dipecahkan dengan metode kasiski karena kunci tidak diulang.

   Kelebihan tahap dua H-Playfair dibanding varian vigenere yang tanpa kunci berulang adalah varian vigenere yang tanpa kunci berulang masih bisa dipecahkan dengan menerka-nerka panjang kuncinya. Ketika panjang kunci yang diterka cocok dengan panjang kunci sebenarnya, plainteks akan dengan mudah didapatkan dengan fungsi substitusi balikan. Tahap ke-dua H-Playfair memiliki mekanisme substitusi tidak biasa sehingga perlu diketahui posisi-posisi huruf kunci pada kotak 6x6 untuk memecahkan cipherteks.

   Kelihatannya dengan tahap dua saja, algoritma H-Playfair sudah tangguh. Namun, teknik distribusi kemunculan setiap 36 huruf mampu memecahkan algoritma ini.

   Oleh karena itu, tahap dua perlu dikombinasikan dengan tahap pertama agar dapat mengatasi kelemahan-kelemahan tadi.

   Untuk memecahkan kombinasi tahap pertama dan tahap kedua ini harus dilakukan percobaan *brute force* mencari kunci. Banyaknya cara untuk memecahkan kunci H-Playfair adalah 36! cara.

   Jadi, H-Playfair memiliki sifat *confusion* (membingungkan). Sebagai bukti, lihat contoh pada langkah H-Playfair tahap dua yang telah diberikan.

   plainteks: `sa ya he ba`
   cipherteks1: `tn xn br cd`
   cipherteks2: `55 gn 43 01`

   huruf a tidak selalu berasosiasi dengan huruf yang sama. Begitu pula untuk pasangan huruf, pasangan huruf yang sama belum tentu menghasilkan pasangan huruf cipherteks yang sama.

2) Diffusion
   Pengubahan satu karakter plainteks dapat menyebabkan perubahan semua karakter cipherteks setelahnya. Pada tahap dua H-Playfair dilakukan substitusi tanpa kunci berulang lalu substitusi selanjutnya (untuk plainteks yang lebih panjang dari panjang kunci) berdasarkan cipherteks hasil tahap pertama sehingga statistik kemunculan huruf/karakter dan statistik hubungan plainteks dan cipherteks menjadi sulit diprediksikan.

3.2. Kelemahan algoritma kriptografi H-Playfair

Kelemahan algoritma kriptografi H-Playfair adalah pembangkitan kuncinya. Panjang kunci ditentukan sebanyak 36 huruf/karakter dengan setiap hurufnya berbeda sehingga pengguna sulit mencari kunci yang mudah diingat untuk digunakan kembali pada saat dekripsi.

Kelemahan ini bisa saja diatasi dengan pemangkasan huruf-huruf yang berulang dari kalimat yang mudah diingat. Namun, apabila hasil pemangkasan kurang dari 36 karakter, maka timbul masalah baru. Bila karakter sisa diisi secara *default*, penyerang menjadi lebih mudah memecahkan cipherteks hasil enkripsi.

Metode lain untuk menutupi kelemahan tadi adalah dengan cara membangkitkan secara acak deret karakter untuk menempati kotak 6x6 tersisa yang kemudian disimpan didalam header plainteks.

Kunci pun dibatasi tidak boleh lebih dari 36 karakter sehingga kompleksitas algoritma terbatas sebatas itu. Namun, jika diinginkan, dengan memasukkan kelebihan kunci ke kunci untuk tahapan ke-dua, maka

masalah ini bisa diselesaikan.

3.3. Keamanan algoritma kriptografi H-Playfair

Algoritma kriptografi H-Playfair dikatakan relatif aman dibanding algoritma kriptografi klasik lainnya karena memenuhi sifat-sifat :

1) Algoritma kriptografi relatif kompleks. Pemecahan secara analitik sulit dilakukan, sulit mencari hubungan statistik antara plainteks dan cipherteks.
2) Waktu tercepat yang diperlukan untuk memecahkan H-Playfair apabila untuk membangkitkan satu buah kunci satu milidetik adalah 36! milidetik.
3) Biaya untuk memecahkan algoritma ini lebih tinggi dibanding algoritma klasik lainnya.

3.4. Analisis serangan terhadap H-Playfair

3.4.1. *Exhaustive attack* atau *brute force attack*

Serangan ini adalah mencoba semua kemungkinan kunci. Setiap plainteks yang diketahui dienkripsi dengan kunci terkaan untuk dicocokkan dengan cipherteks pasangannya.

Kunci masukkan untuk algoritma kriptografi H-Playfair memiliki panjang 36 karakter. Oleh karena itu, serangan ini mencoba kunci sebanyak 36! untuk mendapatkan posisi-posisi yang cocok untuk huruf (a,b,c,d,…,z) dan angka (0,1,2,3,…,9).

3.4.2. *ciphertext-only attack*

Pendeduksian untuk mendapatkan P_{i+1} dari $C_{i+1} = Ek(P_{i+1})$ tidak berguna dilakukan karena plainteks selanjutnya sulit dipecahkan tidak bisa ditentukan hanya dari cipherteks yang diketahui. Tidak ada

3.4.3. *known-plaintext attack*

Prinsip *known-plaintext attack* adalah menerka plainteks dari pasangan cipherteksnya yang bersesuaian akibat pesan yang memiliki format yang terstruktur. H-Playfair mencegah kemungkinan ini karena pada H-Playfair, untuk kata-kata yang sama berkemungkinan kecil mempunyai cipherteks yang sama pula, teratasi pada tahap dua enkripsi H-Playfair. Penduga bisa saja menduga suatu kata pada pesan yang terstruktur, tetapi dugaan itu hanya sebatas beberapa kata dan itupun hanya berupa terkaan yang sulit untuk dibuktikan.

3.4.4. *chosen-plaintext attack*

Sama halnya dengan *ciphertext-only attack*, serangan ini tidak mampu mematahkan algoritma kriptografi H-Playfair. H-Playfair tidak menyebabkan adanya korelasi antara cipherteks dan plainteks.

3.4.5. *adaptive-chosen-plaintext attack*

Serangan ini merupakan kasus khusus untuk serangan *chosen-plainteks attack* sehingga serangan ini pun sulit melumpuhkan H-Playfair.

3.4.6. *chosen-ciphertext attack*

Jika cipherteks diketahui, maka plainteks yang telah dienkripsi oleh H-Playfair tetap sulit dicari. Jenis serangan ini tidak cocok untuk algoritma H-Playfair karena kunci pun tidak bersifat public.

3.4.7. Teknik distribusi frekuensi pasangan huruf

Dengan bantuan komputer, frekuensi pasangan huruf hasil enkripsi algoritma kriptografi H-Playfair adalah sebagai berikut (yang ditampilkan adalah frekuensi pasangan yang memiliki distribusi tertinggi):

Table 1 : tabel distribusi kemunculan pasangan huruf cipherteks (dihitung dari 5018 pasangan huruf pesan bahasa inggris)

pasangan	distribusi	pasangan	distribusi
ER	6	GK	4
TR	6	1M	4
YE	5	NO	4
WA	5	CF	4
FG	5	4R	4
HB	5	E6	4
VE	5	RU	4
X2	5	SA	4
QX	5	UL	4
RI	5	8U	4
GW	5	93	4
OP	5	O1	4
LU	4	FJ	4
TD	4	8P	4
WB	4	P3	4
K0	4	22	4
JE	4	J2	4
BY	4	LL	4
UT	4	QQ	3
H9	4	R7	3

Jika dibandingkan dengan distribusi frekuensi pasangan huruf pada bahasa inggris, maka tidak dapat dicari plainteks yang sebenarnya.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini antara lain:

1. H-Playfair mengatasi kelemahan pada playfair biasa yang bisa dipecahkan dengan teknik frekuensi ganda.
2. H-Playfair aman untuk digunakan, relatif lebih aman dari algoritma kriptografi klasik biasa.
3. Serangan biasa sulit mematahkan algoritma

ini, kecuali dengan menggunakan pencarian kunci.

4. algoritma kriptografi H-Playfair tidak bisa dipecahkan dengan teknik frekuensi distribusi ganda.

DAFTAR REFERENSI

[1] Munir, Rinaldi. (2006). "Diktat Kuliah IF5054 Kriptografi", Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika , Institut Teknologi Bandung.

[2] Bishop, David, Introduction to Cryptography with Java Applets, Grinnell college, 2003

H-Playfair Cipher

Hasanul Hakim / NIM : 13504091 [1)]
1) Program Studi Teknik Informatika ITB, Bandung,
email: if14091@students.if.itb.ac.id, haha_3030@yahoo.com

Abstract *– Playfair Cipher memiliki banyak kelemahan. Playfair Cipher dapat diserang dengan menggunakan teknik frekuensi distribusi huruf ganda pada suatu bahasa. Selain itu, Playfair Cipher tidak menyertakan huruf J sehingga bisa menimbulkan ambiguitas pada saat dekripsi.*
H-Playfair Cipher termasuk kedalam polygram cipher, salah satu tipe dari cipher subtitusi. H-Playfair Cipher adalah algoritma kriptografi yang mampu mengatasi kelemahan algoritma playfair biasa. H-Playfair Cipher menambah langkah algoritma Playfair biasa ditambah kunci diperluas menjadi bujursangkar 6x6. Tambahan langkah memiliki kemiripan dengan varian vigenere, tetapi fungsi penambahannya berbeda.
Makalah ini membahas tentang algoritma H-Playfair, keamanan H-Playfair, kekuatan dan kelemahan H-Playfair, serta kriptanalisis terhadap H-Playfair. Kriptanalisis yang dilakukan meliputi exhaustive attack, metode exhaustive key search, ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, adaptive-chosen-plaintext attack, chosen-ciphertext attack, dan teknik analisis frekuensi.

Kata Kunci*: H-Playfair cipher, playfair cipher, polygram cipher, kriptanalisis, kriptografi.*

1. PENDAHULUAN

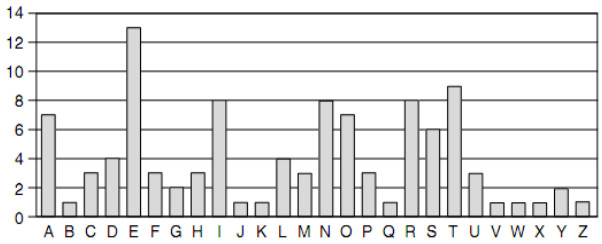
Playfair cipher adalah cipher klasik yang ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair[1]. Kekuatan dari algoritma ini adalah pada kuncinya yang menyusun bujursangkar 5x5. Kemungkinan kunci : 25! = 15.511.210.043.330.985.984.000.000.

Namun, playfair cipher bisa dipecahkan dengan teknik frekuensi distribusi ganda yaitu teknik yang menghitung frekuensi kemunculan pasangan dua huruf cipherteks yang kemudian dibandingkan dengan frekuensi pasangan dua huruf pada suatu bahasa. Disamping itu, hasil dekripsi playfair dapat menimbulkan ambiguitas karena saat enkripsi plainteks, semua huruf J pada plainteks diganti terlebih dahulu dengan huruf I.

Serangan-serangan yang mungkin dihadapi terhadap algoritma kriptografi H-Playfair antara lain:

1. *Exhaustive attack*
2. *Ciphertext-only attack*
3. *Known-plaintext attack*
4. *Chosen-plaintext attack*
5. *Adaptive-chosen-plaintext attack*
6. *Chosen-ciphertext attack*
7. Teknik analisis frekuensi

Teknik analisis frekuensi adalah teknik yang membandingkan distribusi kemunculan huruf pada *ciphertext* terhadap distribusi kemunculan huruf pada berbagai teks suatu bahasa. Lanjutannya adalah teknik analisis frekuensi pasangan huruf. Teknik analisis frekuensi pasangan huruf membandingkan distribusi dua huruf.



Gambar 1 : frekuensi distribusi huruf bahasa inggris[2]

Frekuensi kemunculan pasangan huruf dalam bahasa inggris dapat didekati dengan penghitungan pengalikan distribusi kemunculan sebuah huruf dengan distribusi huruf pasangannya. Jadi jika melihat pada gambar 1, frekuensi kemunculan pasangan huruf tertinggi adalah pasangan huruf ‘t’ dan ‘e’.

Algoritma kriptografi H-Playfair dikatakan aman apabila memenuhi kriteria berikut[1] :

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.
2. Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.
3. Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

2. ALGORITMA H-PLAYFAIR

H-Playfair termasuk kedalam polygram cipher sehingga H-Playfair dikategorikan juga algoritma kriptografi klasik. H-Playfair diciptakan sebagai

varian dari algoritma kriptografi playfair untuk mengatasi kelemahan playfair.

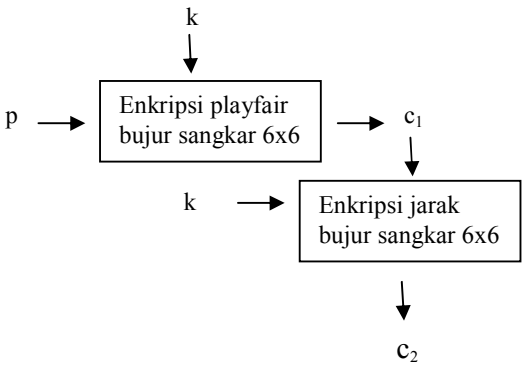
Kunci H-Playfair adalah 26 huruf (a,b,c,d,…,z) ditambah 10 buah angka (0,1,2,3,...,9) yang disusun di dalam bujur sangkar 6x6. Setiap bujur sangkar berisi huruf yang berbeda satu sama lain.

Contoh kunci :

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

Gambar 2: kunci H-Playfair

Algoritma enkripsi H-Playfair terdiri dari dua tahap. Yang pertama melakukan algoritma enkripsi sama dengan algoritma enkripsi playfair. Hanya saja bujursangkar berukuran 6x6 dan huruf j tetap ada. Tahap ke-dua melakukan algoritma lanjutan yang memiliki kemiripan dengan varian algorima kriptografi vigenere dengan fungsi substitusi berdasarkan jarak antar huruf di dalam bujursangkar 6x6.



Gambar 3: skema enkripsi H-Playfair

Algoritma enkripsi H-Playfair adalah sebagai berikut :

1) Pesan yang akan dienkripsi dituliskan dalam pasangan huruf. Jika dalam pasangan terdapat huruf yang sama, sisipkan huruf-huruf *dummy*. Jika terdapat huruf yang belum berpasangan, maka pasangkan huruf tersebut dengan *dummy*.

   Contoh plainteks:
   `saya hebat doong.`

   Dummy: DMY, plainteks menjadi :

   `sa ya he ba td od my on gd my`

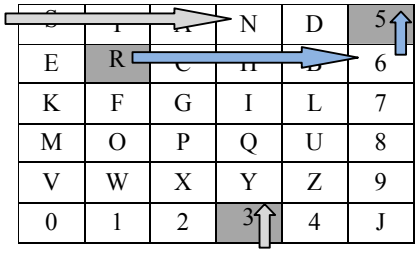
2) Lakukan algoritma seperti algoritma enkripsi playfair untuk mensubstitusikan semua pasangan huruf plainteks dengan bujursangkar kunci 6x6.

   Hasilnya menjadi :
   `tn xn br cd a5 ut qv qt la qv`

3) Hasil enkripsi tadi kemudian dikenakan algoritma enkripsi lanjutan. Huruf hasil enkripsi tadi dipasangkan dengan huruf pertama kunci untuk digantikan menjadi huruf baru menggunakan fungsi enkripsi jarak. Fungsi enkripsi jarak ini adalah menghitung jarak antara huruf yang akan dienkripsi dengan huruf kunci lalu mencari huruf dengan jarak yang sama terhadap kunci.
   Jika panjang kunci telah habis, sisanya diganti dengan huruf-huruf yang akan dienkripsi dari awal.

   contoh :
   plainteks: `tn xn br cd`
   kunci: `st an d5 er` (dari kotak 6x6)
   hasil: `55 gn 43 0l`

   Untuk huruf r dengan kunci 5 menghasilkan karakter 3. Jarak karakter 5 dari karakter r pada kotak adalah 4 petak kanan dan satu petak atas. Sehingga karakter dengan 4 petak kanan dan 1 petak atas dari karakter 5 (kunci) adalah 3 (jika melewati batas atas dan kanan maka definisi satu petak atas adalah karakter paling bawah pada kotak 6x6 pada kolom yang sama dan karakter paling kiri pada kotak 6x6 pada baris yang sama).



Gambar 4 : karakter r dan kunci 5 menghasilkan 3

Algoritma dekripsi kebalikan dari enkripsi yakni :

1) Cari karakter-karakter yang berjarak dari karakter kunci sama dengan karakter kunci ke cipherteks.
2) Lalu lakukan algoritma dekripsi playfair
3) Hilangkan dummy.

3. KRIPTANALISIS

3.1. Kekuatan algoritma kriptografi H-Playfair

Meskipun H-Playfair termasuk algoritma kriptografi klasik, tetapi kemampuan H-Playfair setara dengan kemampuan algoritma kriptografi modern yang memiliki prinsip membingungkan (*confusion)* dan menyebar (*diffusion)* [1].

Prinsip Shannon yang dipenuhi H-Playfair:

1) Confusion
   H-Playfair menyembunyikan hubungan antara cipherteks dan plainteks. Tidak seperti *caesar cipher* yang setiap huruf yang sama diganti menjadi huruf yang sama pula. Begitu pula dengan algoritma kriptografi playfair, yang setiap dua huruf yang sama diganti menjadi dua huruf yang sama pula.

   Prinsip *confusion* dapat terpenuhi karena pada H-Playfair dilakukan enkripsi dua tahap, kedua tahap saling berbeda.

   Tahap pertama seperti tahapan enkripsi playfair yang masih bisa dipecahkan dengan teknik frekuensi kemunculan pasangan huruf.

   Tahap kedua mirip seperti varian vigenere tanpa kunci yang diulang-ulang untuk substitusi, tetapi penambahan huruf kunci dengan huruf plainteks ke-dua (hasil enkripsi tahap pertama H-Playfair) bergantung pada posisi huruf-huruf pada kotak kunci 6x6. Tahap ke-dua tidak bisa dipecahkan dengan metode kasiski karena kunci tidak diulang.

   Kelebihan tahap dua H-Playfair dibanding varian vigenere yang tanpa kunci berulang adalah varian vigenere yang tanpa kunci berulang masih bisa dipecahkan dengan menerka-nerka panjang kuncinya. Ketika panjang kunci yang diterka cocok dengan panjang kunci sebenarnya, plainteks akan dengan mudah didapatkan dengan fungsi substitusi balikan. Tahap ke-dua H-Playfair memiliki mekanisme substitusi tidak biasa sehingga perlu diketahui posisi-posisi huruf kunci pada kotak 6x6 untuk memecahkan cipherteks.

   Kelihatannya dengan tahap dua saja, algoritma H-Playfair sudah tangguh. Namun, teknik distribusi kemunculan setiap 36 huruf mampu memecahkan algoritma ini.

   Oleh karena itu, tahap dua perlu dikombinasikan dengan tahap pertama agar dapat mengatasi kelemahan-kelemahan tadi.

   Untuk memecahkan kombinasi tahap pertama dan tahap kedua ini harus dilakukan percobaan *brute force* mencari kunci. Banyaknya cara untuk memecahkan kunci H-Playfair adalah 36! cara.

   Jadi, H-Playfair memiliki sifat *confusion* (membingungkan). Sebagai bukti, lihat contoh pada langkah H-Playfair tahap dua yang telah diberikan.

   plainteks: `sa ya he ba`
   cipherteks1: `tn xn br cd`
   cipherteks2: `55 gn 43 01`

   huruf a tidak selalu berasosiasi dengan huruf yang sama. Begitu pula untuk pasangan huruf, pasangan huruf yang sama belum tentu menghasilkan pasangan huruf cipherteks yang sama.

2) Diffusion
   Pengubahan satu karakter plainteks dapat menyebabkan perubahan semua karakter cipherteks setelahnya. Pada tahap dua H-Playfair dilakukan substitusi tanpa kunci berulang lalu substitusi selanjutnya (untuk plainteks yang lebih panjang dari panjang kunci) berdasarkan cipherteks hasil tahap pertama sehingga statistik kemunculan huruf/karakter dan statistik hubungan plainteks dan cipherteks menjadi sulit diprediksikan.

3.2. Kelemahan algoritma kriptografi H-Playfair

Kelemahan algoritma kriptografi H-Playfair adalah pembangkitan kuncinya. Panjang kunci ditentukan sebanyak 36 huruf/karakter dengan setiap hurufnya berbeda sehingga pengguna sulit mencari kunci yang mudah diingat untuk digunakan kembali pada saat dekripsi.

Kelemahan ini bisa saja diatasi dengan pemangkasan huruf-huruf yang berulang dari kalimat yang mudah diingat. Namun, apabila hasil pemangkasan kurang dari 36 karakter, maka timbul masalah baru. Bila karakter sisa diisi secara *default*, penyerang menjadi lebih mudah memecahkan cipherteks hasil enkripsi.

Metode lain untuk menutupi kelemahan tadi adalah dengan cara membangkitkan secara acak deret karakter untuk menempati kotak 6x6 tersisa yang kemudian disimpan didalam header plainteks.

Kunci pun dibatasi tidak boleh lebih dari 36 karakter sehingga kompleksitas algoritma terbatas sebatas itu. Namun, jika diinginkan, dengan memasukkan kelebihan kunci ke kunci untuk tahapan ke-dua, maka

masalah ini bisa diselesaikan.

3.3. Keamanan algoritma kriptografi H-Playfair

Algoritma kriptografi H-Playfair dikatakan relatif aman dibanding algoritma kriptografi klasik lainnya karena memenuhi sifat-sifat :

1) Algoritma kriptografi relatif kompleks. Pemecahan secara analitik sulit dilakukan, sulit mencari hubungan statistik antara plainteks dan cipherteks.
2) Waktu tercepat yang diperlukan untuk memecahkan H-Playfair apabila untuk membangkitkan satu buah kunci satu milidetik adalah 36! milidetik.
3) Biaya untuk memecahkan algoritma ini lebih tinggi dibanding algoritma klasik lainnya.

3.4. Analisis serangan terhadap H-Playfair

3.4.1. *Exhaustive attack* atau *brute force attack*

Serangan ini adalah mencoba semua kemungkinan kunci. Setiap plainteks yang diketahui dienkripsi dengan kunci terkaan untuk dicocokkan dengan cipherteks pasangannya.

Kunci masukkan untuk algoritma kriptografi H-Playfair memiliki panjang 36 karakter. Oleh karena itu, serangan ini mencoba kunci sebanyak 36! untuk mendapatkan posisi-posisi yang cocok untuk huruf (a,b,c,d,…,z) dan angka (0,1,2,3,…,9).

3.4.2. *ciphertext-only attack*

Pendeduksian untuk mendapatkan P_{i+1} dari $C_{i+1} = Ek(P_{i+1})$ tidak berguna dilakukan karena plainteks selanjutnya sulit dipecahkan tidak bisa ditentukan hanya dari cipherteks yang diketahui. Tidak ada

3.4.3. *known-plaintext attack*

Prinsip *known-plaintext attack* adalah menerka plainteks dari pasangan cipherteksnya yang bersesuaian akibat pesan yang memiliki format yang terstruktur. H-Playfair mencegah kemungkinan ini karena pada H-Playfair, untuk kata-kata yang sama berkemungkinan kecil mempunyai cipherteks yang sama pula, teratasi pada tahap dua enkripsi H-Playfair. Penduga bisa saja menduga suatu kata pada pesan yang terstruktur, tetapi dugaan itu hanya sebatas beberapa kata dan itupun hanya berupa terkaan yang sulit untuk dibuktikan.

3.4.4. *chosen-plaintext attack*

Sama halnya dengan *ciphertext-only attack*, serangan ini tidak mampu mematahkan algoritma kriptografi H-Playfair. H-Playfair tidak menyebabkan adanya korelasi antara cipherteks dan plainteks.

3.4.5. *adaptive-chosen-plaintext attack*

Serangan ini merupakan kasus khusus untuk serangan *chosen-plainteks attack* sehingga serangan ini pun sulit melumpuhkan H-Playfair.

3.4.6. *chosen-ciphertext attack*

Jika cipherteks diketahui, maka plainteks yang telah dienkripsi oleh H-Playfair tetap sulit dicari. Jenis serangan ini tidak cocok untuk algoritma H-Playfair karena kunci pun tidak bersifat public.

3.4.7. Teknik distribusi frekuensi pasangan huruf

Dengan bantuan komputer, frekuensi pasangan huruf hasil enkripsi algoritma kriptografi H-Playfair adalah sebagai berikut (yang ditampilkan adalah frekuensi pasangan yang memiliki distribusi tertinggi):

Table 1 : tabel distribusi kemunculan pasangan huruf cipherteks (dihitung dari 5018 pasangan huruf pesan bahasa inggris)

pasangan	distribusi	pasangan	distribusi
ER	6	GK	4
TR	6	1M	4
YE	5	NO	4
WA	5	CF	4
FG	5	4R	4
HB	5	E6	4
VE	5	RU	4
X2	5	SA	4
QX	5	UL	4
RI	5	8U	4
GW	5	93	4
OP	5	O1	4
LU	4	FJ	4
TD	4	8P	4
WB	4	P3	4
K0	4	22	4
JE	4	J2	4
BY	4	LL	4
UT	4	QQ	3
H9	4	R7	3

Jika dibandingkan dengan distribusi frekuensi pasangan huruf pada bahasa inggris, maka tidak dapat dicari plainteks yang sebenarnya.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini antara lain:

1. H-Playfair mengatasi kelemahan pada playfair biasa yang bisa dipecahkan dengan teknik frekuensi ganda.
2. H-Playfair aman untuk digunakan, relatif lebih aman dari algoritma kriptografi klasik biasa.
3. Serangan biasa sulit mematahkan algoritma

ini, kecuali dengan menggunakan pencarian kunci.

4. algoritma kriptografi H-Playfair tidak bisa dipecahkan dengan teknik frekuensi distribusi ganda.

DAFTAR REFERENSI

[1] Munir, Rinaldi. (2006). "Diktat Kuliah IF5054 Kriptografi", Program Studi Teknik Informatika Sekolah Teknik Elektro dan Informatika , Institut Teknologi Bandung.

[2] Bishop, David, Introduction to Cryptography with Java Applets, Grinnell college, 2003