Modifikasi *Playfair Cipher* Dengan Kombinasi *Cipher* Transposisi

Laksito Anindyo [1)]

1) Jurusan Teknik Informatika ITB, Jl. Ganesha 10 Bandung 40132, email: if14122@students.if.itb.ac.id

Abstract – *Playfair Cipher, salah satu Playfair cipher termasuk ke dalam polygram cipher yang merupakan salah satu tipe dari cipher substitusi. Playfair cipher menggunakan 25 buah huruf yang disusun di dalam bujursangkar 5x5 dengan menghilangkan huruf J dari abjad. Setiap elemen bujur sangkar berisi huruf yang berbeda satu sama lain. Dengan semakin berkembangnya teknologi dan pengetahuan kriptografi, kini sebuah PC baru yang dijual di pasaran dengan software tertentu dapat memecahkan sebuah pesan yang dienkripsi menggunakan Playfair cipher dalam hitungan detik Dengan metode analisis frekuensi pasangan pun algoritma ini dapat dipecahkan dengan cukup mudah. Makalah ini membahas perancangan sebuah algoritma yang merupakan modifikasi dari Playfair Cipher. Algoritma ini dirancang sedemikian rupa dan digabungkan dengan algoritma cipher transposisi serta algoritma cipher substitusi biasa dengan menggunakan enkripsi cipher berulang. Algoritma ini kemudian akan kita namakan Super Playfair Cipher..*

Kata Kunci*: Kriptografi klasik, Algoritma, cipher subtitusi, cipher transposisi, Playfair Cipher, analisis frekuensi pasangan.*

1. PENDAHULUAN

Sebelum adanya komputer, kriptografi dilakukan berbasis karakter dengan hanya menggunakan kertas dan pena. Algoritma kriptografi yang digunakan saat itu termasuk dalam sistem kriptografi kunci simetri dan digunakan jauh sebelum ditemukannya sistem kunci publik. Algoritma kriptografi yang berbasis karakter biasanya termasuk dalam salah satu dari *cipher* substitusi, *cipher* transposisi, atau *Super* enkripsi yang merupakan gabungan dari *cipher* substitusi dan *cipher* transposisi.

Jika berbicara mengenai kriptografi klasik, pastilah banyak yang sudah mengetahui *Playfair Cipher*, salah satu algoritma kunci simetri yang menerapkan metode polygram *cipher*. Algoritma ini dipopulerkan oleh Lyon *Playfair*, tetapi sesungguhnya ditemukan oleh Charles Wheatstone pada tahun 1854. *Playfair cipher* digunakan oleh tentara Inggris pada saat Perang Boer (Perang Dunia I). Algoritma ini kini sudah tak banyak digunakan karena telah dengan mudah dapat dipecahkan menggunakan analisis uji frekuensi.

Makalah ini membahas perancangan sebuah algoritma yang merupakan modifikasi dari *Playfair Cipher*. Algoritma ini diberi nama *Super Playfair Cipher*. Algoritma ini diberi nama demikian karena dirancang sedemikian rupa sehingga menjadi sebuah algoritma *Super* enkripsi.

2. *PLAYFAIR CIPHER*

Pada awal penemuannya tahun 1854, *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.

Contoh kunci:

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

Dari papan kunci tersebut, jumlah kemungkinan kunci adalah
25!=15.511.210.043.330.985.984.000.000

Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

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

Baris ke-6 = baris ke-1
Kolom ke-6 = kolom ke-1

Penambahan susunan kunci pada kolom keeenam dan baris keenam dimaksudkan untuk mempermudah dalam melakukan proses penyandian.

2.1 Algoritma 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.

Contoh plainteks:
IT IS FULL MOON! MEET ME AT HAMMERSMITH BRIDGE TONIGHT

- Hilangkan semua karakter yang bukan alfabet.
- Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf.
- Jika ada huruf yang sama pasangan huruf (*bigram*), maka tambahkan huruf X ditengahnya.

Plainteks yang telah dilakukan pengaturan:
IT IS FU LX LM OX ON ME ET ME AT HA MX ME RS MI TH BR ID GE TO NI GH TX

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 (pada kunci yang telah diperluas).

2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang telah 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.

4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini

Contoh kunci (yang telah diperluas)

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

Plainteks : IT IS FU LX LM OX ON ME ET ME AT HA MX ME RS MI TH BR ID GE TO NI GH TX

Chipperteks : DM GZ BZ PY KV TR MR OI DO OI MA QO TN OI YF ZM OP FX GW ED AT IM EL BD

Enkripsi IT menjadi DM ditunjukkan dalam gambar papan kunci berikut ini :

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

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

2.2 Algoritma Dekripsi *Playfair Cipher*

Algoritma dekripsi merupakan kebalikan dari algoritma enkripsi. Caranya, untuk setiap pasangan huruf cipherteks, tentukan titik sudut empat persegi panjang yang terbentuk dari pasangan huruf cipherteks sedangkan dua huruf pada titik sudut yang lain menyatakan pasangan huruf plainteksnya. Urutan huruf pada pasangan plainteks tersebut mengikuti arah empat persegipanjang yang dibentuk pleh pasangan huruf cipherteks.

3. PERANCANGAN *SUPER PLAYFAIR CIPHER*

Secara umum, algoritma *Super Playfair cipher* merupakan gabungan dari algoritma *Playfair cipher* dan algoritma *cipher* transposisi, serta dengan menerapkan enkripsi *cipher* berulang.

Kunci yang digunakan pada algoritma ini terdiri dari kunci bujur sangkar, serta kunci yang berbentuk angka .
Kunci dapat dibentuk dari sebuah kalimat yang mudah diingat, misalnya :
PASUKAN PERANG

Hitung jumlah huruf yang ada (tanpa spasi) sebagai kunci angka : 13

Buang huruf yang berulang dan huruf J jika ada :
PASUKNERG

Lalu tambahkan huruf-huruf yang belum ada (kecuali J) :

PASUKNERGBCDFHILMOQTVWXYZ

Masukkan ke dalam bujur sangkar :

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

3.1 Algoritma Enkripsi *Super Playfair Cipher*

Algoritma enkripsi sebagai berikut :

1. Geser plainteks sejauh kunci angka dengan menggunakan *cipher* substitusi (*Caesar cipher*).
   Jika kunci angka = 13, maka ubah huruf A menjadi huruf N, B menjadi O, C menjadi P, dan seterusnya.

   Dengan mengkodekan setiap huruf abjad dengan *integer* sebagai berikut : A = 0, B = 1, …, Z = 25, maka secara matematis *Caesar cipher* menyandikan plainteks p_1 menjadi c_1 dengan kunci *k* sesuai aturan :
   $c_1 = E(p_1) = (p_1 + k) \bmod 26$

   Contoh :
   Plainteks :
   RAHASIA JANGAN DIBOCORKAN
   Cipherteks :
   ENUNFVN WNATNA QVOBPBEXNA

2. Lakukan enkripsi dengan menggunakan *cipher* transposisi.

   Untuk membuat enkripsi menjadi lebih rumit, kunci sebaiknya tidak lebih dari 9. Jika kunci terdiri dari 2 digit, maka kunci baru = digit 1 + digit 2.
   Contoh : kunci = 13, maka kunci baru = 1+3 = 4.

   Untuk mengenkripsi dengan *cipher* transposisi, teks hasil dari langkah (1) ditulis secara horizontal dengan lebar huruf tetap selebar kunci (dalam kasus ini = 4).

   ```
   E N U N
   F V N W
   N A T N
   A Q V O
   B P B E
   X N A
   ```

   Dibaca secara vertikal menjadi :
   EFNABXNVAQPNUNTVBANWNOE

3. Langkah berikutnya adalah melakukan enkripsi dengan metode *Playfair cipher* seperti telah dijabarkan sebelumnya.
   Jika masukannya adalah : EFNABXNVAQPNUNTVBANWNOE
   Maka *cipher*teksnya menjadi : RD EP RZ CP UM NC PG LZ EK EV RL RW

4. Langkah 1-3 diulang sebanyak n kali dengan n = kunci angka, dengan menggunakan kunci bujursangkar yang digeser sejauh 1 kotak.
   Misal : kunci asli adalah :

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

   Maka kunci pada perulangan berikutnya akan menjadi :

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

   Begitu seterusnya hingga sebanyak n kali..

3.2 Algoritma Dekripsi *Super Playfair Cipher*

Untuk mendapatkan plainteks, akan dilakukan proses dekripsi oleh penerima pesan. Prosesnya sebagai berikut:

1. Geser bukursangkar kunci sejauh *k* kotak, dengan *k* adalah kunci angka.

2. Lakukan dekripsi dengan menggunakan metode *Playfair cipher*.

3. Lakukan dekripsi dengan menggunakan metode *cipher* transposisi.
   Untuk mendekripsi pesan, kita membagi panjang cipherteks dengan panjang kunci. Pada contoh ini kita membagi 23 dengan 4 (pembulatan ke atas) untuk mendapatkan 6.
   Caranya adalah dengan menuliskan kembali cipherteks dalam baris-baris selebar *k* karakter.
   ```
   E F N A B X
   N V A Q P N
   U N T V B A
   N W N O E
   ```

   Lalu dengan membaca setiap kolom, maka kita akan memperoleh pesan semula.
   ENUNFVNWNATNAQVOBPBEXNA

4. Lakukan deskripsi dengan menggunakan *Caesar cipher*.
   Dengan menggunakan fungsi dekripsi :
   $p_1 = D(c_1) = (c_1 - k) \bmod 26$

5. Ulang langkah 2-4 dengan terlebih dahulu

menggeser kotak kunci ke kiri.

3.3 Perbandingan cipherteks hasil modifikasi dengan sebelum modifikasi

Setelah melakukan proses-proses di atas, dapat dilihat bahwa dengan digunakannya modifikasi *Playfair cipher* yang telah dimodifikasi maka cipherteks akan lebih rumit karena terdapat kombinasi dengan algoritma *Caesar cipher* dan *cipher* transposisi, ditambah lagi dengan penggunaan *cipher* berulang dengan kunci yang berubah-ubah membuat semakin sulit.

3.4 Analisis

Analisis hasil program yang dilakukan disini adalah dengan cara melakukan perbandingan antara plainteks yang dienkripsi dan kemudian didekripsi untuk mengembalikan menjadi plainteks kembali.

Dari pengujian yang dilakukan, diketahui bahwa plainteks awal yang enkripsi kemudian didekripsi kembali memiliki kesamaan, namun karakter yang bukan merupakan huruf, alfabet seperti angka, tanda baca, dan spasi menjadi hilang.

Hal tersebut diakibatkan oleh ketidakmampuan algoritma untuk melakukan substitusi terhadap karakter selain huruf alfabet.

Selain itu, jika jumlah karakter pada plainteks ganjil, maka karakter terakhir pada plainteks hasil dekripsi menjadi tidak bermakna.

Untuk segi keamanan, *Playfair cipher* cenderung lemah terhadap serangan-serangan kriptanalis terutama analisis frekuensi. Karena itu dilakukan modifikasi terhadap *Playfair Cipher* sehingga memberi kekuatan tersendiri pada cipherteks sehingga sulit untuk dikriptanalis. Sedangkan *Caesar Cipher* lebih mudah lagi untuk dipecahkan dengan menggunakan teknik analisis frekuensi.

Dengan menggabungkan ketiga jenis algoritma *cipher* ini disertai dengan perulangan, maka hasil yang didapatkan akan lebih rumit dan lebih sulit untuk dipecahkan oleh kriptanalis.

4. KESIMPULAN

Setelah dilakukan pembahasan dan percobaan selama untuk membuat makalah ini, penulis dapat mengambil kesimpulan, yaitu:

1. *Playfair cipher* baik yang orisinil maupun hasil modifikasi dapat menyandikan pesan sehingga hanya pihak yang berhak saja yang dapat melihat isi pesan.

2. *Playfair Cipher* yang telah dimodifikasi menjadi *Super Playfair cipher* adalah solusi yang lebih baik daripa*Playfair cipher* orisinil dalam mengatasi masalah keamanan dan kerahasian data teks.

3. Pada algoritma kriptografi *Playfair Cipher* terdapat kelemahan dalam pendistribusian kunci antara pengirim pesan dan penerima pesan karena algoritma ini menggunkan kunci simetri dalam proses penyandian (enkripsi dan dekripsi).

4. *Super Playfair Cipher* memiliki tingkat keamanan yang lebih tinggi daripada *Playfair Cipher* Orisinil karena proses enkripsinya yang lebih rumit, kunci yang berubah-ubah, serta turut diterapkannya algoritma *cipher* transposisi.

5. Proses penyandian dengan *Super Playfair Cipher* dapat divariasikan dengan mengubah urutan pada algoritma enkripsi dan dekripsi.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] http://www.simonsingh.net/The_Black_Chamber/*Playfaircipher*.htm

[3] http://www.bryson.ltd.uk/cgi-bin/*Playfair*