Modifikasi *Rail Fence Cipher* Menggunakan *Vigenere Cipher*

Tara Baskara – 135 04 042
Jurusan Teknik Informatika ITB, Bandung, email: if14042@students.if.itb.ac.id

Abstraksi – *Seiring meningkatnya perkembangan dunia teknologi, sistem pengamanan yang canggih terhadap suatu data semakin dibutuhkan. Hal ini juga didorong oleh semakin maraknya kejahatan di dunia maya. Salah satu sektor yang rawan mengundang kejahatan adalah sektor pengamanan data. Oleh karena itu, pengguna teknologi semakin beramai-ramai mengembangkan suatu sistem pengamanan terhadap data yang biasa disebut kriptografi. Salah satu metode kriptografi yang dikenal adalah algoritma kriptografi klasik dimana metode ini sudah dikenal sejak lama. Algoritma kriptografi klasik memiliki berbagai macam bentuk, dimana yang akan dibahas dalam makalah ini adalah Rail Fence Cipher dan Vigenere Cipher. Dalam makalah ini, penulis akan mencoba mengembangkan algoritma Rail Fence Cipher dengan menggabungkannya dengan Vigenere Cipher. Modifikasi pada Rail Fence Cipher dilakukan dengan menambahkan kerumitan menggunakan kerterurutan abjad dan Vigenere Cipher digunakan untuk menambah kerumitan dari algoritma. Isi dari makalah meliputi konsep dasar,implementasi dan tingkat keamanan algoritma yang disertai pengujian sederhana.*

Kata Kunci*: Rail Fence Cipher, Vigenere Cipher, enkripsi, dekripsi, plainteks, cipherteks, metode Kasiski, exhaustive key search.*

1 PENDAHULUAN

Sebagai makluk sosial komunikasi merupakan hal yang paling dekat dengan kita. Komunikasi dapat kita artikan sebagai berbagi pikiran, informasi dan intelijen. Segala bentuk aktivitas yang dilakukan oleh seseorang dengan tujuan menyampaikan pesannya pada orang lain merupakan tujuan komunikasi., Dilatarbelakangi oleh kebutuhan manusia tersebut, teknologi komunikasi dewasa ini maju dengan pesat. Dengan kemajuan teknologi tersebut, manusia dapat melakukan pengiriman pesan dengan mudah dimana saja dan kapan saja dengan menggunakan berbagai media.

Perkembangan dunia *digital* saat ini membuat lalu lintas pengiriman pesan/data semakin pesat. Data yang dipertukarkan pun juga bervariasi baik dari jenisnya maupun tingkat kerahasiannya. Mulai dari data pribadi, data organisasi sampai data negara yang sangat rahasia. Hal inilah yang menuntut adanya pengamanan data tersebut sehingga tidak sampai tersadap pihak ketiga. Hingga kini telah banyak ditemukan teknik-teknik dalam pengamanan data, baik teknik klasik maupun modern

Salah satu algoritma kriptografi klasik yang cukup populer adalah *transposition cipher*. *Transposition Cipher* ini memiliki berbagai macam bentuk dan algoritma, diantara contoh dari *cipher* transposisi ini adalah *Rail Fence Cipher*, *Route Cipher* dan *Columnar Cipher*.

Selain itu ada algoritma kriptografi klasik yakni *Subtitution Cipher*. Ini adalah tipe enkripsi pesan yang intinya adalah mengubah isi dari pesan dengan teks lain. Salah satunya adalah *Vigenere Cipher*.

2 DASAR TEORI

2.1 Rail Fence Cipher

Rail Fence Cipher merupakan salah satu variasi implementasi *cipher* transposisi. Pada *Rail Fence Cipher*, plainteks dituliskan secara vertikal ke bawah sepanjang n-*rails*, dan menulis lagi ke kolom baru ketika telah mencapai karakter ke-n. Cipherteks yang dihasilkan adalah urutan karakter yang dibaca secara horizontal. Sebagai contoh, kita mempunyai n=3 dan sebuah pesan
WE ARE DISCOVERED FLEE AT ONCE , maka ditulis :

W	R	I	O	R	F	E	O	E	X
E	E	S	V	E	L	A	N	X	X
A	D	C	E	D	E	T	C	X	X

Karakter tambahan di akhir cipherteks sengaja dibubuhkan diantaranya untuk melengkapi cipherteks sehingga melengkapi blok dan atau untuk mengelabui kriptanalis. Pesan tersebut kemudia dibaca

WRIOR FEOEX EESVE LANXX ADCED ETCXX

Penulisan pesan menjadi blok-blok standar, biasanya sepanjang 5 karakter, dilakukan untuk memudahkan pentransmisian pesan pada telegraf. Algoritma *Rail Fence Cipher* ini tidak terlalu kuat, kemungkinan kunci-kunci yang dipakai terlalu kecil sehingga kriptanalis dapat mencobanya semua dengan manual.

2.2 Vigenere Cipher

Vigenere Cipher menggunakan bujursangkar *vigenere* untuk memperoleh cipherteks dengan menggunakan

kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang penggunaannya (periodik). Bila panjang kunci adalah m, maka periodenya dikatakan m.

Sebagai contoh, jika plainteks adalah "BUNUHDIA" dan kunci adalah "TARA", maka penggunaan kunci secara periodik adalah sebagai berikut :

Plainteks : B U N U H D I A
Kunci : T A R A T A R A

Setiap kunci plainteks dienkripsi dengan setiap huruf kunci di bawahnya.

Untuk melakukan enkripsi dengan *Vigenere Cipher*, lakukan pada bujursangkar *vigenere* sebagai berikut : tarik garis vertikal dari huruf plainteks ke bawah, lalu tarik garis mendatar dari huruf kunci ke kanan. Perpotongan kedua garis tersebut menyatakan huruf cipherteksnya. Sebagai contoh di atas, tarik garis vertikal dari huruf B dan tarik garis mendatar dari huruf T, perpotongannya adalah kotak yang berisi huruf U.

	a	*b*	*c*	*d*	*e*
a	A	B	C	D	E
b	B	C	D	E	F
c	C	D	E	F	G
d	D	E	F	G	H
e	E	F	G	H	I
f	F	G	H	I	J
g	G	H	I	J	K
h	H	I	J	K	L
i	I	J	K	L	M
j	J	K	L	M	N
k	K	L	M	N	O
l	L	M	N	O	P
m	M	N	O	P	Q
n	N	O	P	Q	R
o	O	P	Q	R	S
p	P	Q	R	S	T
q	Q	R	S	T	U
r	R	S	T	U	V
s	S	T	U	V	W
t	T	**U**	V	W	X
u	U	V	W	X	Y
v	V	W	X	Y	Z
w	W	X	Y	Z	A
x	X	Y	Z	A	B
y	Y	Z	A	B	C
z	Z	A	B	C	D

Tabel 1. Enkripsi huruf B dengan T

Hasil enkripsi seluruhnya adalah sebagai berikut :

Plainteks : B U N U H D I A

Kunci : T A R A T A R A

Cipherteks : U U E U A D Z A

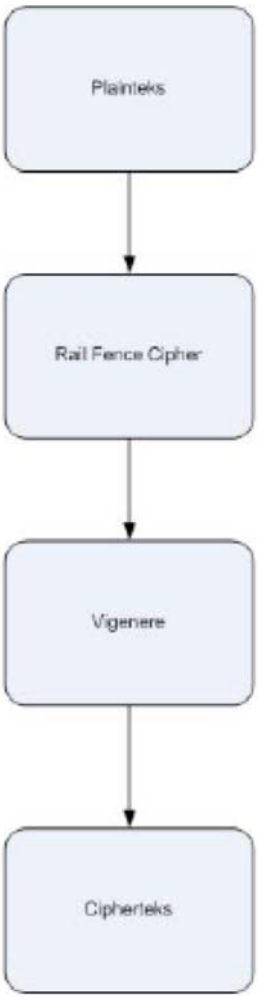
Dekripsi pada vigenere cipher dilakukan dengan cara yang berkebalikan, yaitu menarik garis mendatar dari huruf kunci sampai ke huruf cipherteks yang dituju, lalu dari huruf cipherteks tarik garis vertikal ke atas sampai huruf plainteks.

3 HASIL DAN PEMBAHASAN

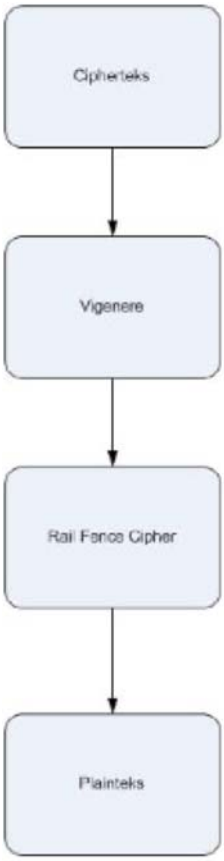
3.1 Perancangan enkripsi Modifikasi *Rail Fence Cipher* menggunakan *Vigenere Cipher*

Modifikasi yang dilakukan penulis dalam makalah ini adalah dengan menggunakan *Rail Fence Cipher* yang telah dimodifikasi oleh penulis dan selanjutnya menggunakan *Vigenere Cipher*.

Sebagai penjelasan , proses enkripsi dan dekripsi pada dapat dilihat pada bagan pada gambar berikut:



Gambar 1. Bagan enkripsi hasil modifikasi



Gambar 2. Bagan dekripsi hasil modifikasi

Penggunaan modifikasi *Rail Fence Cipher* dan *Vigenere Cipher* dalam melakukan proses enkripsi plainteks dapat dilihat pada contoh berikut:

Kita mempunyai pesan "MAAF LAHIR BATIN" dengan kunci "IBU" maka dilakukan proses sebagai berikut :

1. Melakukan enkripsi dengan *Rail Fence Cipher* yang telah dimodifikasi, ditulis

I	M	F	H	B	I
B	A	L	I	A	N
U	A	A	R	T	X

Karakter tambahan di akhir cipherteks sengaja dibubuhkan diantaranya untuk melengkapi cipherteks sehingga melengkapi blok dan atau untuk mengelabui kriptanalis. Pesan tersebut kemudia dibaca berdasarkan keterurutan abjad, dalam contoh di atas kunci IBU berarti dibaca sesuai urutan abjad yaitu BIU sehingga pesan menjadi

ALIAN MFHBI AARTX

Penulisan pesan menjadi blok-blok standar, biasanya sepanjang 5 karakter, dilakukan untuk memudahkan pentransmisian pesan pada telegraf.

2. Melakukan enkripsi dengan *Vigenere Cipher*
Vigenere Cipher menggunakan tabel *Vigenere* atau tabula recta untuk melakukan proses enkripsinya. Dalam program yang penulis rancang, algoritma enkripsi *Vigenere Cipher* menggunakan rumus:

Ci ≡ (Pi + Ki) mod 26

Untuk melakukan enkripsi gunakan rumus diatas dimana i merupakan huruf ke-n dalam plainteks. Untuk i = 1,

C1 ≡ (P1 + K1) mod 26

= (P'A' + K'm') mod 26

= (0 + 12) mod 26

= 12

C'M' = 12

Maka hasil enkripsi *Vigenere Cipher* adalah:

Plainteks : ALIAN MFHBI AARTX

Kunci : IBUIB UIBUI BUIBU

Maka diperoleh cipherteks hasil enkripsi sebagai berikut: IMICO GNIVQ BUZUR

3.2 Perancangan dekripsi *Modifikasi Rail Fence Cipher* menggunakan *Vigenere Cipher*

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

1. Melakukan dekripsi dengan *Vigenere Cipher*
Digunakan rumus :

Pi ≡ (Ci - Ki) mod 26

Proses ini menggunakan himpunan yang sama seperti proses enkripsi. Apabila Ci < Ki, maka Ci = Ci + 26.

Sehingga dengan menggunakan contoh diatas

Chiperteks : IMICO GNIVQ BUZUR
Kunci : IBUIB UIBUI BUIBU
Plainteks : ALIAN MFHBI AARTX

2. Melakukan dekripsi dengan *Rail Fence Cipher*
Dengan menggunakan kata kunci "IBU", kita dapat mendekripsi cipherteks menjadi plainteks.

a) Pertama, tuliskan kembali cipherteks menjadi satu deretan *string*/karakter

ALIANMFHBIAARTX

b) Kemudian, bagi pesan tersebut menjadi blok dengan ukuran sama dan mempunyai jumlah blok sama dengan panjang kunci

ALIAN MFHBI AARTX

Karena terdapat 15 karakter, dan kita tahu bahwa panjang kunci ada 3, kita membagi

blok menjadi 3 dengan panjang masing-masing blok adalah 5

c) Langkah selanjutnya adalah mengurutkan kunci sesuai dengan abjad. Dalam kasus ini kunci adalah IBU dan jika diurutkan sesuai abjad menjadi BIU dan blok-blok diatas sesuai dengan kunci yang diurutkan,

ALIAN = B
MFHBI = I
AARTX = U

Kemudian diurutkan kembali menjadi IBU sehingga blok-blok ikut berubah menjadi

MFHBI = I
ALIAN = B
AARTX = U

d) Langkah terakhir, tulis karakter pertama dari blok ke-1,blok ke-2,blok ke-3 diikuti dengan karakter kedua dari blok ke-1,blok ke-2,blok ke-3 sampai karakter ke-n.

MAAFLAHIRBATINX

e) Sekarang pilah-pilah karakter dari pesan sehingga dapat mudah dibaca,hilangkan karakter *dummy*, dan kode pun telah berhasil didekripsi

3.3 Perbandingan cipherteks hasil modifikasi dengan sebelum modifikasi

Setelah melakukan proses-proses di atas, dapat dilihat bahwa dengan digunakannya modifikasi terhadap *Rail Fence Cipher* yang telah dimodifikasi maka cipherteks akan lebih rumit karena ada permainan urutan abjad disana, ditambah lagi dengan penggunaan *Vigenere Cipher* yang menambah kerumitan terhadap kriptanalis yang akan memecahkan kode ini.

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.

Dengan menggunakan contoh sebelumnya, pesan "MAAF LAHIR BATIN" dienkripsi dengan program menggunakan kunci "IBU" dan menghasilkan cipherteks

IMICOGNIVQBUZUR

Cipherteks ini kemudian didekripsi kembali oleh program menggunakan kunci yang sama, dan menghasilkan plainteks

MAAFLAHIRBATINX

Huruf X ini muncul akibat pengaturan yang dilakukan sebelum pesan dienkripsi dengan algoritma *Rail Fence Cipher*. Huruf X tersebut tidak dapat dihapus karena tidak dapat diketahui apakah huruf tersebut merupakan hasil pengaturan atau merupakan bagian dari pesan. Misalnya ada pesan "FIND BOX" dengan kunci "AIR" maka setelah dienkripsi dan didekripsi menggunakan program akan didapat FINDBOXXX. Jika program ditambahkan fungsi untuk menghapus huruf X, maka pesan akan berubah menjadi FINDBO, berbeda dengan pesan asli.

Untuk segi keamanan, *Rail Fence Cipher* cenderung lemah terhadap serangan-serangan kriptanalis terutama analisis frekuensi. Karena itu dilakukan modifikasi terhadap *Rail Fence Cipher* sehingga memberi kekuatan tersendiri pada cipherteks sehingga sulit untuk dikriptanalis. Sedangkan untuk *Vigenere Cipher* lebih mudah untuk dipecahkan dengan adanya metode Kasiski. Metode ini membantu menemukan panjang kunci. Setelah panjang kunci diketahui, maka langkah berikutnya adalah menentukan kata kunci dengan menggunakan *exhaustive key search*.

4 KESIMPULAN

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

1. *Rail Fence Cipher* merupakan salah satu teknik kriptografi klasik yang menggunakan pergeseran posisi dengan menggunakan kata kunci sebagai inti dari algoritma untuk enkripsi dan dekripsi teks.
2. *Vigenere Cipher* ditambahkan setelah plainteks dienkripsi menggunakan *Rail Fence Cipher*, menambah kerumitan tersendiri terhadap proses enkripsi dan dekripsi.
3. Modifikasi terhadap *Rail Fence Cipher* dengan *Vigenere Cipher* menghasilkan cipherteks yang lebih rumit dan sulit dipecahkan karena ada modifikasi permainan abjad pada *Rail Fence Cipher* dan dipersulit dengan tambahan dari *Vigenere Cipher*.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006.

[2] Forouzan, Behrouz, *Cryptography and Network Security*, McGraw-Hill, 2008.

[3] http://en.wikipedia.org/wiki/Rail_fence