Vigènere Cipher dengan Modifikasi Bujursangkar Vigènere menggunakan Kode Morse

Ahmad Zamakhsyari Sidiq [1)]
1) Jurusan Teknik Informatika ITB, Jl. Ganesha 10, email: zamakhsyari135@students.itb.ac.id

Abstract – *Vigènere Cipher adalah salah satu jenis kriptografi klasik yang cukup populer dan banyak dipakai. Vigènere Cipher diperkenalkan oleh Blaise de Vigènere pada tahun 1586. Vigènere Cipher termasuk dalam polyalphabetic subtitusion cipher, yaitu mengubah plainteks dengan kunci tertentu yang diulang sampai memiliki panjang sama dengan plainteks tersebut untuk mendapatkan cipherteks. Namun cipher ini memiliki kelemahan bisa dipecahkan dengan metode Kasiski untuk mendapatkan panjang kunci dan kemudian dilakukan analisis frekuensi untuk mendapatkan kunci tesebut. Untuk mengatasi kelemahan tersebut penulis mencoba untuk melakukan modifikasi terhadap algoritma Vigènere Cipher dengan melakukan perubahan pada bujursangkar Vigènere. Bujursangkar Vigenere dirubah menggunakan Kode Morse yang dibangkitkan dari kunci. Kode Morse adalah sistem komunikasi yang dilakukan dengan merubah huruf, angka dan tanda baca menjadi titik dan garis, biasanya digunakan dalam telegraf. Dikembangkan oleh Samuel FB Morse pada awal abad ke-19. Pada dasarnya, metode ini akan melakukan pembobotan nilai pada setiap huruf sesuai kode morse. Tiap titik akan diberi nilai 1 dan garis diberi nilai 2. bujursangkar Vigenere akan digeser sesuai jumlah yang dihasilkan dari kunci. Dengan metode ini diharapkan usaha pemecahan kode melalui metode kasiski dan analisis frekuensi akan menghasilkan kunci yang salah sehingga plainteks tidak akan didapatkan.*

Kata Kunci*: Vigènere chiper, Morse, Kriptografi, Polyalphabetic Subtitusion Cipher*

1. PENDAHULUAN

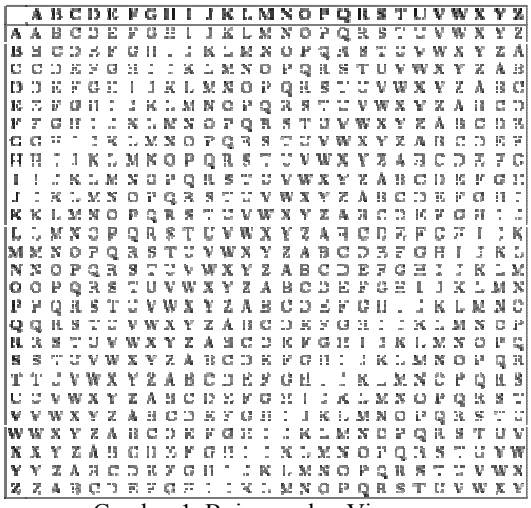
Dalam kriptografi klasik, ada dua jenis algoritma yang sering dipakai, yaitu Cipher Substitusi dan Cipher Transformasi. Cipher Substistusi bekerja dengan mengganti setiap karakter dari pesan (plainteks) dengan karakter lain dalam alphabet. Cipher Subtitusi sendiri memiliki banyak jenis, dan salah satunya adalah cipher substitusi abjad majemuk (polyalphabetic subtitusion cipher). Dalam cipher substitusi abjad majemuk, setiap huruf dalam plainteks dikodekan berbeda bergantung pada posisi mereka dalam plainteks.Cipher abjad-majemuk dibuat dari sejumlah cipher abjad-tunggal, masing-masing dengan kunci yang berbeda.

2. DASAR TEORI

1.1. Vigenere Cipher

Vigenere cipher adalah salah satu dari jenis algoritma klasik yang mengunakan substitusi abjad majemuk. Vigènere Cipher diperkenalkan oleh Blaise de Vigènere pada tahun 1586, namun algoritma tersebut baru dikenal luas 200 tahun kemudian. Penggunaan Algoritma Vigenere yang paling terkenal adalah ketika Algoritma ini digunakan oleh Tentara Konfederasi pada Perang Sipil Amerika[1].

Vigenere cipher bekerja dengan menggunakan Bujursangkar Vigenere (Gambar 1) untuk melakukan proses enkripsi dan dekripsi.



Gambar 1: Bujursangkar Vigenere

Kolom paling kiri pada bujursangkar Vigenere menyatakan huruf-huruf kuncinya sedangkan pada baris paling atas menyatakan huruf-huruf pada plainteks.

Bujursangkar Vigenere digunakan untuk memperoleh cipherteks dengan menggunakan kunci. Jika kunci lebih pendek dari panjang plainteks maka kunci diulang sampai panjangnya sama dengan plainteks. pengulangan ini disebut sistem periodik.

Enkripsi pada Vigenere cipher bisa ditulis dalam

bentuk operasi:

$$C_i \equiv (P_i + K_i) \mod 26$$

Dan proses dekripsi dengan menggunakan bentuk operasi :

$$P_i \equiv (C_i - K_i) \mod 26$$

Contoh Singkat:

Sebagai contoh, plainteks "COME AT HOME" dengan kunci "TEXT". Karena panjang kunci lebih pendek dari plainteks, maka kunci diulang secara periodik. Jadi diperoleh:

```
PT: COME AT HOME
KEY:text te xtte
CT: VSJX TX EHFI
```

Untuk melakukan dekripsi, maka proses yang dilakukan merupakan kebalikan dari proses enkripsi. Dengan menggunakan contoh di atas, diketahui bahwa chiperteks adalah VSJX TX EHFI dengan kunci tent. Karakter plainteks dapat dengan mudah diperoleh dengan cara mencari huruf chiperteks pada baris huruf kunci yang bersesuaian pada badan bujursangkar vigenere, maka diperoleh huruf plainteks yang merupakan perpotongan dari kolom plainteks.

Bila dicermati, setiap huruf hasil enkripsi pada Vigenere Chiper merupakan Caesar Chiper dengan kunci yang berbeda-beda. Contoh:

C('C') = ('C' + 't') mod 26 = V

C('T') = ('H' + 'x') mod 26 = E

Huruf yang sama tidak selalu dienkripsi menjadi huruf chiperteks yang juga sama. Seperti yang terlihat pada contoh di atas, huruf plainteks M dapat dienkripsi menjadi J atau F, tergantung kunci. Inilah yang menjadi karakteristik utama dari chiper abjad-majemuk di mana setiap huruf plainteks dapat memiliki kemungkinan banyak huruf chiperteks

Vigenere cipher ini bisa dipecahkan dengan menggunakan metode Kasiski dan analisis frekuensi.

2.2 Metode Kasiski

Metode ini sebenarnya terlebih dahulu telah dikembangkan oleh Charles Babbage pada tahun 1854. Namun Vigenere Cipher baru bisa dipecahkan oleh Friedrich Kasiski pada tahun 1863dengan menggunakan metode ini, yang kemudian diberi nama sesuai namanya. Metode ini bisa menemukan panjang kunci dari suatu plainteks memanfaatkan pengulangan pasangan 2 huruf atau lebih. Pengulangan pada cipherteks ini terjadi oleh karena kunci yang sama diterapkan pada karakter plainteks yang sama menghasilkan pengulangan pada hasil chiperteks. Interval munculnya pengulangan pada chiperteks kemudian dapat difaktorkan dan dapat mengindikasikan kunci beserta panjangnya yang digunakan dalam proses enkripsi[1].

Apabila terdapat beberapa pengulangan yang relatif panjang pada chiperteks, maka intervalnya dihitung mulai dari karakter pertama dari pengulangan sampai ketemu dengan karakter pengulangan yang sama berikutnya. Faktor terbesar dari nilai interval ini merepresentasikan panjang karakter kunci yang digunakan untuk mengenkripsi pesan.

Berikut adalah contoh singkat:

```
 Cipherteks : IZGSV PFQBW RAGBP
WQBWR ARUNZ DPGLJ LUOPR NOUOD LJ
```

Pemfaktoran:

Pengulangan	Interval	Faktor	Faktor terbesar
QBWRA	9	3, 3	3
LJ	12	2, 2, 3	3
UO	6	2, 3	3

Metode ini membutuhkan frekuensi pengulangan yang cukup banyak agar memudahkan proses identifikasi faktor. Hal ini tentu saja menyulitkan apabila pesan ternyata sangat singkat sehingga jarang atau bahkan tidak ditemukan pengulangan sama sekali. Namun, terkadang pada pesan yang panjang sekalipun metode ini gagal untuk mengidentifikasi pengulangan.

2.3. Morse

Kode Morse adalah sistem komunikasi yang dilakukan dengan merubah huruf, angka dan tanda baca menjadi titik dan garis, biasanya digunakan dalam telegraf.[2] Dikembangkan oleh Samuel Finely Breese Morse (1791-1872) pada awal abad ke-19. Kode Morse ini pertama kali berhasil diujicobakan antara Washington DC dan Baltimore pada tanggal 24 Mei 1844.[3] Pada kode morse internasional, titik direpresentasikan dengan menekan sebentar tombol switch pada telegraf, sehingga bisa ditekan berulang-ulang secara cepat. Sedangkan titik direpresentasikan dengan menekan tombol lebih lama sehingga tidak mungkin ditekan lagi dengan cepat.

Kode morse di representasikan sebagai berikut:

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

Tabel 1. Huruf dalam Morse

Angka	Morse
1	**.----**

2	**..---**
3	**…--**
4	**….-**
5	**…..**
6	**-….**
7	**--…**
8	**----..**
9	**----.**
0	**-----**

Tabel 2. Angka dalam Morse

3. RANCANGAN ALGORITMA/ MODIFIKASI VIGENERE

Implementasi Kode Morse dalam memodifikasi bujursangkar vigenere adalah dengan memberikan bobot pada kunci yang dimasukan pengguna. Pembobotan dilakukan dengan aturan:

1. Titik diberi nilai 1
2. Garis diberi nilai 2

Daftar bobot tiap huruf bisa dilihat dalam tabel 3.

Huruf	Morse	Bobot
A	**.-**	1+2 = 3
B	**-...**	2+1+1+1 = 5
C	**-.-.**	2+1+2+1 = 6
D	**-..**	2+1+1 = 4
E	**.**	1
F	**..-.**	1+1+2+1 = 5
G	**--.**	2+2+1 = 5
H	**....**	1+1+1+1 = 4
I	**..**	1+1 = 2
J	**.---**	1+2+2+2 = 7
K	**-.-**	2+1+2 = 5
L	**.-..**	1+2+1+1 = 5
M	**--**	2+2 = 4
N	**-.**	2+1 = 3
O	**---**	2+2+2 = 6
P	**.--.**	1+2+2+1 = 6
Q	**--.-**	2+2+1+2 = 7
R	**.-.**	1+2+1 = 4
S	**...**	1+1+1 = 3
T	**-**	2
U	**..-**	1+1+2 = 4
V	**...-**	1+1+1+2 = 5
W	**.--**	1+2+2 = 5
X	**-..-**	2+1+1+2 = 6
Y	**-.--**	2+1+2+2 = 7
Z	**--..**	2+2+1+1 = 6

Tabel 3. Pembobotan Huruf berdasarkan Morse

Cara menghitung bobot suatu kunci adalah dengan menggunakan persamaan:

$B = K \bmod 26$ (1)

Kemudian setelah kunci didapatkan besar bobotnya, misalnya B, maka pada bujur sangkar vigenere dilakukan modifikasi yakni dengan menggeserkan kolom terkiri pada tabel (kolom kunci) sebanyak B dan menggeser baris teratas (baris plainteks) sebanyak B juga. Kolom digeser kebawah dan baris digeser kesebelah kanan. Dengan ini, ciphertext yang akan dihasilkan menjadi benar-benar berbeda dengan yang dihasilkan oleh bujursangkar vigenere biasa, selain itu kriptanalis akan kesulitan untuk mencoba memecahkan karena tidak mengetahui bujursangkar mana yang digunakan.

3. HASIL DAN PEMBAHASAN

3.1 Pembahasan

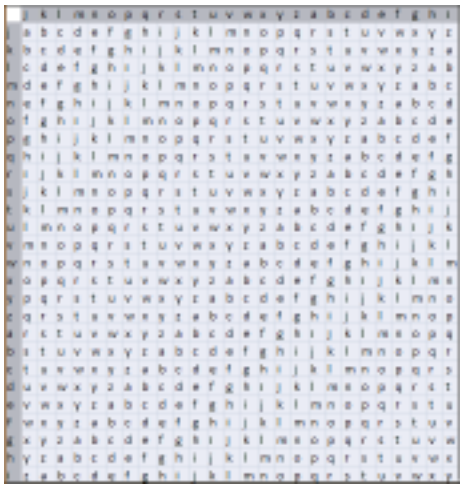
Plainteks berikut akan coba dikodekan dengan algoritma baru ini.

> An Information System (IS) is the system of persons, data records and activities that process the data and information in a given organization, including manual processes or automated processes.

Misalkan kunci yang digunakan adalah "TESTING". Dengan persamaan 1 kita bisa dapatkan bobot dari kunci "TESTING" adalah :

B = (2+1+3+1+2+3+5) mod 26 = 17 mod 26 = 17

Bobot yang didapatkan adalah 17, sehingga tabel mengalami pergeseran, hasil pergeseran bisa dilihat pada gambar 3.



Gambar 2. Hasil Pergeseran Bujursangkar Vigenere

Cipherteks yang dihasilkan adalah :

> Ay Hnuiemlsidh Fydseb CF id sht mlsedm dz cecrocm, qaez rtwbror acx ncehvxnved shpn crzbehm ghp caiu nno hnuiemlsidh vn l fikya ocfaccmaehoc, cacwtdxht mlmupf crzbehmrs zq ajnbmlses jeondshyf.

Sedangkan cipherteks yang dihasilkan oleh yang bujursangkar vigenere biasa adalah:

Tr Agnbxfelbwa Yrwlxu VY bw lam felxwf ws vxvkhvf, jtxs kmpukhk tvq gvxaoqgoxw laig vksuxaf zai vtbn ggh agnbxfelbwa og e ybdrt hvytvvftxahv, vtvpmwqam fefniy vksuxafkl sj tcgufelxl cxhgwlary.

3.2 Pengujian Algoritma

Pengujian yang dilakukan adalah dengan menggunakan vigenere.nb yang berasal dari, http://mywebpages.comcast.net/
kehebatan vigenere.nb ini telah terbukti dengan pemecahan cipherteks berikut. Vigenere.nb berhasil menebak tepat kuncinya yaitu BLAZE.

DZLNRFWRNWTDTHPMHOQIBYEWTSPSRMPYW
GMDSSGSXPDSLFAONVPAIMMPYWGMDSHDLB
OFNVNPDNJNJCNQQLNHSODAAMMTTXFVEIRE
XMYSLFTNRTFNTNVTQABIUSASLJDASXFYTHS
OSACFFPNJIFYLXESZURIEJOTGPYSHHFCTGEUE
OAIJXPNVULNSLFLSJIEPXBIFOIMKMJSNMTEHD
VFLNXTPTNSXPHHHGIJOTAPFLCAJDHSSECAVQ
ZLTSIOEINRUZTGIDFRHSVDIMGJOEMXPQTGIE
ZGHRUSEMMHSTSMNPTGIEZGCMEYOSLJYGHR
USEMMHSTSMNPTGEUHARXIPCTVJZURMONIC
IOERDQBCKDHTSEQPPNKGSMXER

hasilnya adalah

colonelrossstillworeanexpressionwhichshowed
thepooropinionwhichhehadformedofmycompanions
abilitybutisawbytheinspectorsfacethathis
attentionhadbeenkeenlyarousedyouconsiderthat
tobeimportantheaskedexceedinglysoisthereanypoint
towhichyouwouldwishtodrawmyattentionto
thecuriousincidentofthedoginthenighttimethe
dogdidnothinginthenighttimethatwasthecurious
incidentremarkedsherlockholmes

Dari pengujian pada situs tersebut, menghasilkan kunci WHVWLQJ. Vigenere.nb berhasil menemukan panjang yang benar namun tidak berhasil menemukan kunci yang tepat.

4. KESIMPULAN

Dari pembahasan mengenai modifikasi algoritma yang dilakukan diatas, ada beberapa kesimpulan yang bisa diambil, yaitu: Algoritma baru ini tidak mempengaruhi pada metode kasiski, metode kasiski masih bisa menebak dengan tepat panjang kunci, namun metode ini tidak bisa menemukan kunci yang benar karena tabel yang digunakan dirubah dan tidak diketahui besar perubahannya.

DAFTAR REFERENSI

[1] R. Munir, "Diktat Kuliah IF5054", Program Studi Teknik Informatika Institut Teknologi Bandung, 2006.
[2] http://www.pramuka-jaksel.org/
[3] http://www.rod.beavon.clara.net/morse.htm
http://www.webtitanic.net/frameterms.html
http://hem.passagen.se/tan01/poly.html
http://www.trincoll.edu/depts/cpsc/cryptography/vigenere.html
http://mywebpages.comcast.net/