Vigenère Cipher dengan Pergeseran Karakter Kunci, Penambahan Angka, dan Pergeseran Karakter pada Baris Plain Teks

Prasetyo Nugroho [1)]
1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if14039@students.if.itb.ac.id

Abstract – *Makalah ini membahas tentang modifikasi pada Vigenère Cipher dengan menambah karakter angka, menggeser urutan huruf dan angka pada baris plainteks, dan menggeser karakter kunci setiap perulangannya. Hal tersebut dilakukan untuk memperkuat algoritma ini dan mempersulit untuk memecahkan cipherteks dengan analisi frekuensi.*

Kata Kunci*: Kriptografi Klasik, Vigenere* Cipher

1. PENDAHULUAN

Perkembangan dunia digital saat ini membuat lalu lintas pengiriman data elektronik semakin ramai dan sensitif. Hampir setiap orang melakukan transaksi data digital setiap hari. Data yang dipertukarkan pun juga bervariasi baik dari jenisnya maupun tingkat kerahasiaannya. Mulai dari data pribadi, data organisasi sampai dengan data negara yang sangat rahasia. Hal inilah yang menuntut adanya pengamanan terhadap proses pengiriman data tersebut sehingga tidak diketahui dan kemudian dimanfaatkan untuk kepentingan pihak ketiga. Telah banyak ditemukan teknik-teknik dalam pengamanan data, baik teknik klasik maupun modern.

Vigenère Cipher adalah salah satu algoritma terbaik dari *cipher* abjad majemuk 'manual'. Dalam melakukan enkripsi dan dekripsi, Vigenère Cipher menggunakan tabel bujursangkar yang ditunjukkan oleh Gambar 1. Kolom paling kiri dari table tersebut menyatakan karakter kunci, sedangkan baris paling atas menyatakan karakter *plain teks*.

Untuk melakukan enkripsi terhadap pesan, digunakan kunci yang berulang. Namun penggunaan tabel yang tetap dan pengunaan kunci yang berulang dapat menjadi suatu kelemahan dari Vigenère Cipher untuk dapat dianalisi oleh seorang kriptanalis untuk memecahkan *cipher teks* tersebut. Dengan melakukan Kriptanalisis dengan metode Kasiski, Vigenère Cipher dapat dipecahkan.

Untuk mengatasi penggunaan tabel yang tetap dan penggunaan kunci yang sama dan berulang, maka dilakukan modifikasi agar tabel dapat berubah sesuai dengan kunci dan pergeseran kunci ditiap perulangannya. Dengan demikian, *cipher teks* yang dihasilkan akan menjadi lebih sulit untuk dianalisis dengan metode analisis frekuensi karena seakan-akan menggunakan kunci yang lebih panjang.

2. RANCANGAN ALGORITMA

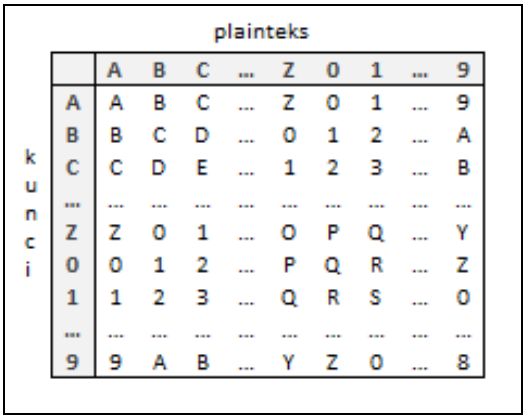
Vigenère Cipher mengenkripsi teks dan menghasilkan *cipher teks* yang hanya mengenkripsi huruf yang terdapat pada teks tersebut. Tabel yang digunakan tetap disetiap mengenkripsi teks. Dalam mengenkripsi teks, apabila panjang kunci kurang dari panjang teks, maka enkripsi dilakukan dengan melakukan subtitusi tiap huruf *plain teks* dengan huruf pada kunci dan kunci digunakan secara berulang-ulang. Hal ini menyebabkan algoritma Vigenère Cipher bisa dipecahkan dengan analisis frekuensi, karena akan ada kemungkinan pasangan huruf yang sama, karena pemakaian kunci yang sama secara berulang-ulang.

Dalam modifikasi algoritma Vigenère Cipher ini, dilakukan penambahan karakter angka, sehingga *plain teks* yang bisa dienkripsi tidak hanya sebatas alfabet saja, melainkan juga angka. Dengan menambahkan karakter angka, ukuran tabel yang digunakan untuk melakukan enkripsi dan dekripsi menjadi lebih besar.

Contoh tabel Vigenère yang telah dimodfikasi ditunjukkan oleh Gambar 2.

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

Gambar 1: Tabel Vigenère



	A	B	C	...	Z	0	1	...	9
A	A	B	C	...	Z	0	1	...	9
B	B	C	D	...	0	1	2	...	A
C	C	D	E	...	1	2	3	...	B
...	...	...	...	...	...	...	...	...	...
Z	Z	0	1	...	O	P	Q	...	Y
0	0	1	2	...	P	Q	R	...	Z
1	1	2	3	...	Q	R	S	...	0
...	...	...	...	...	...	...	...	...	...
9	9	A	B	...	Y	Z	0	...	8

Gambar 2: Tabel modifikasi Vigenère

Selain dengan menambah jumlah karakter tersebut, modifikasi Vigenère Cipher juga dilakukan pada baris *plain teks* pada tebel. Modifikasi yang dilakukan adalah melakukan pergeseran karakter pada baris *plain teks* pada tabel Vigenère, sehingga mempersulit kriptanalis dalam memecahkan *cipher teks*. Pergeseran karakter tersebut dilakukan dengan menjumlahkan tiap karakter kunci dan melakukan modulo dengan 36, dengan ketentuan:

A=0, B=1, …, Z=25, 0=26, …, 9=35 persamaan (1)

dan,

kk mod 36 = s persamaan (2)

dimana *kk* adalah hasil penjumlahan tiap karakter kunci, *s* adalah jumlah pergeseran yang akan dilakukan.
Dengan demikian, apabila kunci = “IF2004” maka dengan mengacu pada “persamaan (1)” dan “persamaan (2),” akan dilakukan pergeseran sebanyak 123 mod 36 = 15. Dengan demikian, *cipher teks* akan lebih sulit untuk dianalisis karena Kriptanalis tidak mengetahui dengan pasti tabel yang digunakan.
Modifikasi terakhir yang dilakukan adalah pergeseran karakter kunci pada setiap perulangan. Pada Vigenère Cipher yang biasa, perulangan penggunaan kunci adalah sebagai berikut:

```
P : KRIPTOGRAFI
K : IF2004IF200
```

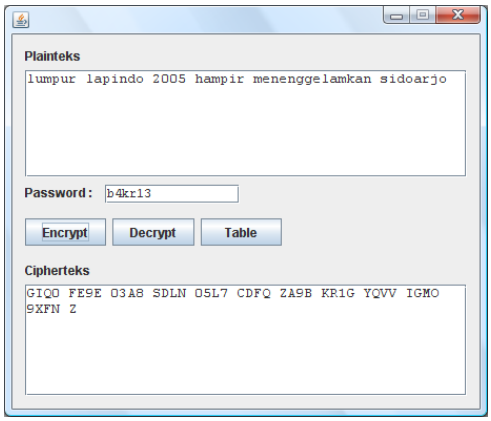
Dimana *P* adalah *Plain teks*, dan *K* adalah *Key*. Dengan melakukan pergeseran karakter kunci disetiap perulangan, maka kunci akan menjadi seperti berikut:

```
P : KRIPTOGRAFI
K : IF2004F2004
```

Pergeseran dilakukan dengan menggeser satu karakter ke kiri, sehingga karakter pertama dari kunci tersebut menjadi karakter terakhir dan karakter kedua dari kunci menjadi karakter pertama. Dengan demikian, kunci seakan-akan menjadi lebih panjang sebanyak 2^n, dengan n adalah panjang kunci. Dengan panjang kunci yang seperti ini, menyebabkan *cipher teks* menjadi lebih sulit untuk dipecahkan dengan metode analisis frekuensi.

3. IMPLEMENTASI DAN PEMBAHASAN

Untuk melihat hasil kerja dari modifikasi Vigenère Cipher ini, maka dilakukan pengujian dengan membuat aplikasi sederhana dengan menggunakan bahasa pemrograman Java dan kakas pemrograman *NetBeans* serta antar muka sebagai berikut:



Gambar 3: Aplikasi Vigenère yang dimodifikasi

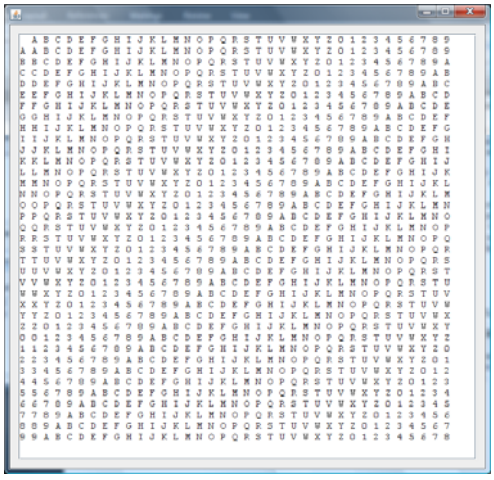
Pengujian dilakukan dengan memasukkan teks ke aplikasi pada *textarea* plainteks dan memasukkan kata kunci ke aplikasi pada *textfield* password. Adapun plain teks (P) dan kunci (K) yang akan digunakan adalah sebagai berikut:

```
P : lumpur lapindo 2005 hampir
    menenggelamkan sidoarjo
K : b4kr13
```

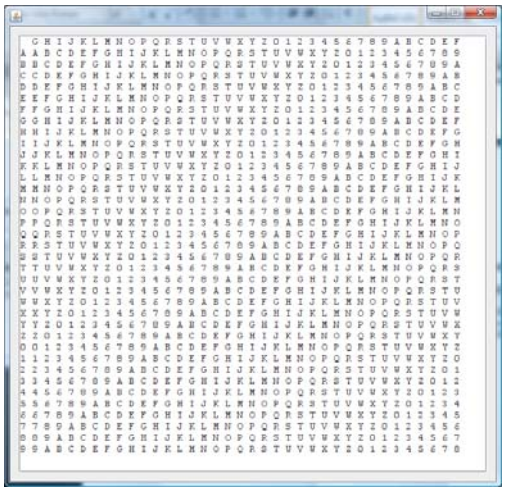
Dengan menggunakan Vigenère Cipher yang telah dimodifikasi, maka hasil dari enkripsi *plain teks* tesebut adalah *cipher teks* (C) sebagai berikut:

```
C : GIQ0 FE9E 03A8 SDLN 05L7 CDFQ ZA9B
    KR1G YQVV IGMO 9XFN Z
```

Hal ini membuktikan bahwa modifikasi pada Vigenère Cipher telah berhasil dalam mengenkripsi teks.
Untuk membuktikan bahwa tabel Vigenère yang digunakan berbeda, tabel yang berlum digeser ditunjukkan pada Gambar 4, dan yang telah digeser ditunjukkan pada Gambar 5.



Gambar 4: Tabel modifikasi Vigenère pada aplikasi



Gambar 5: Tabel modifikasi Vigenere pada aplikasi setelah pergeseran

Pengujian dekripsi pada *cipher teks* (C) dengan kunci (K) dilakukan dengan memasukkan *cipher teks* ke aplikasi pada *textarea* cipherteks dan memasukkan kata kunci ke aplikasi pada *textfield* password. Hasil dekripsi apabila kunci yang digunakan benar adalah sebagai berikut:

```
P :LUMP URLA PIND O200 5HAM PIRM ENEN
   GGEL AMKA NSID OARJ O
```

sedangkan apabila kunci salah adalah sebagai berikut:

```
K :abcd3
P :FGNW LC6A 6274 YCJJ 64J4 ICDN V978
   GXZD UWUS EMLM 53EL W
```

Aplikasi modifikasi Vigenère tidak *case sensitive*, sehingga apabila teks atau kunci yang dimasukkan menggunakan huruf kapital, kecil, atau campuran, hasil *cipher teks* maupun *plain teks* sama sekali tidak terpengaruh.

Algoritma Modifikasi Vigenère ini mempunyai kelemahan yang sama dengan algoritma Vigenère biasa, yaitu apabila menggunakan kunci dengan panjang satu huruf, karena akan membuat algoritma ini menjadi sama seperti algoritma *Caesar Cipher*, yaitu hanya seperti melakukan subtitusi dengan menggeser tiap karakter sebanyak n kali.

4. KESIMPULAN

Algoritma Modifikasi Vigenère Cipher ini lebih baik dari Algoritma Vigenère Cipher biasa karena dapat mengenkripsi teks yang mengandung huruf dan angka. Selain itu, algoritma modifikasi Vigenère Cipher ini juga meningkatkan keamanan data yang dienkripsi karena proses enkripsi yang dilakukan menggunakan kunci sepanjang 2^n dengan n adalah panjang kunci sebenarnya, sehingga analisis frekuensi menjadi lebih sulit untuk dilakukan. Selain dengan menggeser kunci di tiap perulangannya sehingga menjadikan kunci seakan-akan lebih panjang, modifikasi yang dilakukan juga mengubah tabel Vigenère, sehingga tabel selalu berubah berdasarkan kunci yang dipakai. Modifikasi ini dilakukan untuk memperkuat atau meningkatkan tingkat keamanan dalam mengenkripsi data sehingga lebih aman dari enkripsi dari Vigenère biasa.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, 2006.