Modifikasi Pergeseran Bujur Sangkar Vigenere Berdasarkan Susunan Huruf dan Angka pada Keypad Telepon Genggam

Pradita Herdiansyah – NIM : 13504073 [1)]
1)Program Studi Teknik Informatika ITB, Jl. Ganesha 10, Bandung, email: if14073@students.if.itb.ac.id

Abstrak – *Vigenere Cipher merupakan salah satu metode cipher abjad-majemuk (polyalpabethic substitution cipher). Proses enkripsi dan dekripsi yang dilakukan Vigenere Cipher memanfaatkan bujursangkar Vigenere yang memanfaatkan kunci tertentu. Untuk memecahkan kunci tersebut, kriptanalis yang hanya mengetahui ciphertext saja, dapat memanfaatkan metode Kasiski dan dipadu dengan teknik analisis frekuensi. Untuk menghambat kerja kriptanalis tersebut dalam memecahkan kunci, dapat dilakukan modifikasi pada bujur sangkar Vigenere yang digunakan memanfaatkan kunci yang digunakan dalam proses enkripsi dan dekripsi teks. Tiap-tiap huruf pada kata kunci di konversi menjadi angka berdasarkan susunan angka dan huruf yang dapat dilihat pada keypad normal telepon genggam (bukan keypad QWERTY). Seluruh angka yang dihasilkan akan dijumlahkan dan dimodulokan dengan 26 sehingga menghasilkan sebuah angka yang digunakan sebagai ukuran pergeseran deret kunci pada bujursangkar Vigenere. Enkripsi dan dekripsi yang dilakukan akan menggunakan bujursangkar hasil modifikasi tersebut. Dengan modifikasi ini, tidak menutup kemungkinan kriptanalis tetap akan dapat menemukan kunci 'semu' untuk mendapatkan plaintext namun cukup menghambat bagi kriptanalis yang berusaha mencari kunci asli yang umumnya dapat dibaca, sedangkan kunci 'semu' yang didapatkan susunannya akan lebih sulit dibaca, sehingga sulit ditebak oleh kriptanalis.*

Kata Kunci*:Vigenere, cipher, enkripsi, dekripsi, telepon genggam, keypad.*

1. PENDAHULUAN

Belakangan ini kebutuhan komunikasi dan transfer data dapat dikatakan cukup tinggi. Untuk menjaga keamanan, kerahasiaan, serta keabsahan data tersebut, ilmu kriptografi berperan penting dalam penyandian data yang dikomunikasikan tersebut. Salah satu metode dalam kriptografi yang digunakan dalam proses pengamanan data adalah Vigenere Cipher. Vigenere Cipher merupakan salah satu metode algoritma kriptografi klasik yang dirasa cukup aman hingga saat ini.

Untuk memecahkan Vigenere Cipher tersebut, kriptanalis yang hanya mengetahui ciphertext saja, dapat menggunakan metode Kasiski yang digunakan untuk menentukan panjang kunci yang kemudian dilanjutkan dengan teknik analisis frekuensi sehingga akan ditemukan kunci yang digunakan. Untuk mengantisipasi kinerja kriptanalis, dalam Vigenere Cipher, kunci yang paling aman digunakan adalah kunci yang panjangnya sama dengan panjang plaintext yang akan dienkripsi. Namun, mengingat kunci yang cukup panjang akan cukup menyulitkan pengirim maupun penerima, sehingga biasanya kunci yang digunakan tidak akan sepanjang plaintext dan umumnya kunci dapat dibaca (bukan rangkaian huruf yang acak).

Untuk mempersulit kerja kriptanalis dalam memecahkan kata kunci, penulis mengusulkan modifikasi terhadap Vigenere Cipher dengan melakukan pergeseran susunan deret kunci pada bujur sangkar Vigenere. Banyaknya pergeseran yang dilakukan didapat dari konversi huruf-huruf kunci yang digunakan dalam proses enkripsi/dekripsi menjadi angka berdasarkan kesesuaian huruf kunci dengan angka yang terdapat pada keypad telepon.

Dengan modifikasi tersebut, diharapkan kriptanalis akan terhambat ketika mencoba memecahkan dan mendapatkan kunci yang digunakan dengan menggunakan metode Kasiski yang dilanjutkan dengan analisis frekuensi.

2. LANDASAN TEORI

2.1. Vigenere Cipher

Vigenere Cipher ditemukan di Prancis pada abad 16 oleh Blaise de Vigenere yang kemudian dapat dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19.

Untuk melakukan enkripsi dan dekripsi menggunakan Vigenere Cipher, diperlukan bujursangkar Vigenere yang akan digunakan sebagai landasar untuk mengubah plaintext menjadi ciphertext berdasarkan kunci yang digunakan dan sebaliknya. Berikut ini adalah model potongan bujursangkar Vigenere dengan deret horizontal huruf paling atas(kapital-tebal) melambangkan plaintext dan deret vertikal huruf paling kiri (non kapital-tebal) melambangkan kunci:

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

Tabel 1 Potongan Bujur Sangkar Vigenere Plaintext A-J

Jika ada sebuah plaintext misalnya "HONDAACCORD" dienkripsi menggunakan Vigenere Cipher dengan kunci "CAR", maka berdasarkan hasil pembacaan bujursangkar Vigenere

Plaintext : H O N D A A C C O R D
Kunci : C A R C A R C A R C A
akan menghasilkan
Ciphertext : J O E F A R E C F T D

Proses yang sama namun berkebalikan akan dilakukan untuk melakukan dekripsi sebuah ciphertext dengan kunci yang telah dilakukan. Proses dekripsi juga tetap memanfaatkan bujur sangkar Vigenere sebagai panduan untuk mendapatkan plaintext.

Pada dasarnya, enkripsi huruf yang dilakukan pada Vigenere Cipher merupakan Caesar Cipher dengan kunci yang berbeda-beda. Peninjauan dapat dilakukan kembali pada contoh plaintext "HONDAACCORD" dienkripsi dengan kunci "CAR" menghasilkan ciphertext "JOEFARECFTD". Jika dilakukan analisis pada tiap-tiap hurufnya, dapat digambarkan dalam fungsi berikut (diambil contoh huruf pertama dari plaintext "HONDAACCORD"):

c('H') = ('H' + 'c') mod 26 = J

Dengan perhitungan sebagai berikut:

1. Huruf 'H' sebagai plaintext merupakan huruf ke-8 dalam alphabet.
2. Huruf 'c' sebagai huruf kunci yang bersesuaian dengan huruf 'H' merupakan huruf ke-3 dalam alphabet.
3. Hasil enkripsi adalah penjumlahan huruf plainteks dengan kunci dikurangi 1 kemudian dimodulokan dengan 26 akan menghasilkan huruf ciphertext. Dalam kasus ini berarti (8+3-1) mod 26 = 10. Huruf ke-10 dalam alphabet adalah huruf J

Maka secara umum, fungsi enkripsinya dapat ditulis sebagai:

c(H) = (uH + uK - 1) mod26 = uC

Keterangan :
H = huruf plaintext
uH = urutan huruf plaintext pada alphabet
uK = urutan huruf kunci pada alphabet
uC = urutan huruf ciphertext pada alphabet

Sedangkan untuk fungsi dekripsi dapat dicontohkan sebagai berikut:

d('J') = ('J' + 1 – 'c' + 26) mod 26 = H

Maka untuk fungsi dekripsinya secara umum dapat ditulis sebagai:

d(C) = (uC + 1 –uK + 26) mod26 = uH

Keterangan :
C = huruf ciphertext
uH = urutan huruf plaintext pada alphabet
uK = urutan huruf kunci pada alphabet
uC = urutan huruf ciphertext pada alphabet

2.2. Keypad Telepon Genggam

Keypad telepon genggam yang digunakan sebagai panduan konversi dalam modifikasi bujur sangkar Vigenere ini dibatasi hanya keypad konvensional / keypad umum yang terdapat pada rata-rata telepon genggam yang beredar di masyarakat. Keypad telepon genggam yang memiliki format QWERTY yang menyerupai keyboard komputer atau laptop tidak digunakan sebagai panduan disini.

Berikut ini tabel konversi huruf-angka berdasarkan keypad telepon genggam:

Huruf	Angka
A-B-C	2

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

Tabel 2 Konversi Huruf-Angka Berdasarkan Keypad Telepon Genggam

3. HASIL DAN PEMBAHASAN

3.1. Modifikasi Vigenere Cipher Beserta Contoh Pengujiannya

Hal mendasar dalam modifikasi yang dibahas dalam tulisan ini adalah pergeseran susunan huruf kunci pada bujur sangkar Vigenere. Jumlah atau jauh pergeseran yang terjadi didasarkan pada perhitungan hasil konversi huruf kunci menjadi angka menurut format yang terdapat pada keypad telepon genggam. Untuk lebih mudahnya, panduan konversi yang dilakukan dapat dilihat pada Tabel 2.

Proses enkripsi yang sudah dimodifikasi dapat diamati dari contoh sebagai berikut (contoh yang diberikan sama dengan contoh yang telah digunakan sebelumnya agar dapat dibandingkan langsung hasilnya):

1. Plaintext yang diberikan adalah "HONDAACCORD" dan kunci yang digunakan adalah "CAR".
2. Melakukan konversi kunci menjadi angka sesuai format keypad telepon genggam (dapat dilihat di Tabel 2). Kunci "CAR" dikonversikan menjadi "227"
3. Mencari nilai **faktor geser 'G'** dengan menjumlahkan seluruh angka hasil konversi kunci kemudian hasilnya dimodulokan dengan 26
   G = (2+2+7) mod 26 = 11
4. Menggeser susunan huruf kunci pada bujursangkar Vigenere memutar ke arah bawah sebesar faktor gesernya, yakni 11 langkah. Berikut ini model potongan bujur sangar Vigenere yang telah dimodifikasi dengan faktor geser 11.

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

Tabel 3 Potongan Bujur Sangkar Vigenere Plaintext A-J Hasil Modifikasi dengan Faktor Geser 11

Bujur sangkar Vigenere hasil modifikasi tersebut digunakan sebagai panduan dalam enkripsi dan dekripsi dengan mengunakan kunci yang tetap sama yakni "CAR"

Plaintext : H O N D A A C C O R D
Kunci : C A R C A R C A R C A
Maka berdasarkan bujur sangkar hasil modifikasi, ciphertext yang diperoleh adalah
Ciphertext : U Z P Q L C P N Q E O

Modifikasi pada Vigenere Cipher ini dapat digambarkan dalam fungsi enkripsi sebagai berikut:

$c(H) = (uH + uK - 1 + G) \bmod 26 = uC$

Keterangan :
H = huruf plaintext
uH = urutan huruf plaintext pada alphabet
uK = urutan huruf kunci pada alphabet
uC = urutan huruf ciphertext pada alphabet
G = faktor pergeseran

Sedangkan untuk fungsi dekripsi modifikasi pada Vigenere Cipher ini sebagai berikut:
$d(C) = (uC + 1 - uK - G + 26) \bmod 26 = uH$

Keterangan :
C = huruf ciphertext
uH = urutan huruf plaintext pada alphabet

uK = urutan huruf kunci pada alphabet
uC = urutan huruf ciphertext pada alphabet
G = faktor pergeseran

Berikut ini contoh lain dari hasil pengujian yang telah dilakukan menggunakan Vigenere Cipher yang telah dimodifikasi:

Plaintext	: TOYOTASPRINTERTRUENO
Kunci	: DRIFTING
Ciphertext	: JSTGZVSIHMILKMTKKIIG

3.2. Analisis Hasil Modifikasi Vigenere Cipher Terhadap Serangan Kriptanalis

Kriptanalis yang berusaha memecahkan kunci pada Vigenere Cipher umumnya menggunakan metode Kasiski untuk mengetahui panjang kunci yang digunakan. Setelah itu, kriptanalis melanjutkannya dengan teknik analisis frekuensi. Untuk memudahkan pembahasan, perlu kita tinjau kembali contoh plaintext “HONDAACCORD” dengan kunci “CAR”.

Pada pembahasan Vigenere Cipher biasa, kriptanalis akan mendapatkan informasi berupa ciphertext “JOEFARECFTD” saja. Jika diasumsikan bahwa metode Kasiski telah dilakukan pada ciphertext tersebut dan menghasilkan nilai 3 sebagai panjang kunci, maka kriptanalis akan melanjutkan langkah pemecahan kuncinya menuju teknik analisis frekuensi. Teknik analisis frekuensi terkadang tidak menghasilkan langsung huruf-huruf kunci yang tepat berdasarkan indeks frekuensi kemunculan karena tabel indeks kemunculan huruf yang digunakan sebagai pedoman tidak selamanya cocok dengan kemunculan huruf pada plaintext maupun ciphertext. Oleh karena itu, kriptanalis biasanya turut pula menggabungkan metode terkaan untuk mendapatkan kunci yang tepat.Terkaan yang dilakukan bisa dilakukan pada huruf plaintext atau huruf kunci. Berdasarkan teknik analisis frekuensi, misalnya kriptanalis mendapatkan kunci “CAZ”. Huruf kunci Z masih salah, kriptanalis dapat melakukan terkaan untuk mendapatkan kunci yang tepat berdasarkan 2 huruf CA yang sudah benar. Karena biasanya kunci yang digunakan merupakan kata atau kalimat bermakna yang dapat diingat oleh pengirim dan penerima pesan, maka kriptanalis dapat menerka kunci yang tepat misalnya CAT, CAR, atau CAN.

Sedangkan kriptanalis yang berusaha memecahkan kata kunci pada Vigenere Cipher yang dimodifikasi akan mendapatkan informasi berupa ciphertext “UZPQLCPNQEO”. Kriptanalis tidak mengetahui kunci yang digunakan serta nilai faktor pergeserannya sehingga kriptanalis tetap melakukan kriptanalisis berdasarkan Vigenere Cipher standar dengan memanfaatkan bujur sangkar Vigenere yang asli. Setelah kriptanalis memanfaatkan metode Kasiski dan teknik analisis frekuensi, tidak menutup kemungkinan bagi kriptanalis untuk mendapatkan sebuah kunci ‘semu’ yang dapat digunakan untuk melakukan enkripsi atau dekripsi dengan tepat tanpa perlu mengetahui kunci aslinya. Namun, kriptanalis masih mendapatkan penghalang apabila indeks frekuensi kemunculan huruf yang digunakan sebagai panduan ternyata tidak langsung menghasilkan kunci yang tepat. Misalnya saja kriptanalis mendapatkan kunci ‘semu’ NLO dimana huruf O merupakan kunci yang salah. Jika kriptanalis melakukan metode terkaan terhadap kunci, maka kriptanalis akan mengalami kesulitan saat mencari huruf kunci yang tepat karena susunan huruf kunci sudah berubah sehingga kunci ‘semu’ itu menjadi tidak bermakna sehingga terkaan yang dilakukan tidak semudah menerka kunci yang memiliki makna. Dalam kasus ini, kunci ‘semu’ yang tepat adalah NLC

4. KESIMPULAN

Dari hasil pembahasan, analisis, dan pengujian yang telah penulis lakukan, dapat disimpulkan bahwa modifikasi Vigenere Cipher yang berupa pergeseran bujur sangkar Vigenere berdasarkan susunan huruf dan angka pada keypad telepon genggam memiliki kelebihan sebagai berikut:

1. Pengirim dan penerima pesan tidak perlu saing mengirimkan informasi tambahan. Informasi yang dipertukarkan cukup kata kunci yang digunakan saja meskipun proses enkripsi dan dekripsi yang dilakukan berdasarkan tabel Vigenere yang telah dimodifikasi berdasarkan kata kunci tersebut.
2. Nilai faktor pergeseranyang muncul tidak spesifik. Untuk dua buah atau lebih nilai faktor pergeseran yang sama dapat dihasilkan dari 2 atau lebih kunci yang berbeda.
3. Kriptanalis yang berusaha memecahkan kata kunci menggunakan metode Kasiski dan teknik analisis frekuensi tidak dapat langsung mendapatkan kunci yang digunakan. Terlebih lagi jika tabel analisis frekuensi yang digunakan tidak sepenuhnya tepat sehingga memerlukan terkaan untuk mendapatkan kunci yang dimaksud. Kriptanalis memang bisa memperoleh plaintext tanpa perlu mengetahui kunci asli. Kriptanalis bisa mendapatkan plaintext dengan memenfaatkan kunci ‘semu’ saja. Namun, kunci ‘semu’ yang telah mengalami modifikasi yakni pergeseran tersebut tidak lagi bermakna sebagaimana umumnya kunci asli yang bermakna agar memudahkan pengirim dan penerima. Hal ini akan menyulitkan kriptanalis yang menggunakan terkaan untuk membenahi beberapa huruf kunci yang masih salah.

Namun, di lain sisi, modifikasi Vigenere Cipher ini juga memiliki kelemahan sebagai berikut:

1. Jika konversi kunci menjadi angka yang dimodulokan dengan 26 menghasilkan faktor

pergeseran bernilai 0, maka tidak ada perubahan apapun yang terjadi pada Vigenere Cipher.

2. Jika tabel indeks frekuensi yang digunakan oleh kriptanalis pada saat analisis frekuensi sudah benar-benar tepat sehingga kriptanalis tidak perlu menggunakan terkaan terhadap beberapa huruf kunci, maka modifikasi ini menjadi tidak berarti karena kunci ‘semu’ yang didapatkan sudah tepat dan dapat digunakan untuk mendekripsi ciphertext yang ada dengan benar.

DAFTAR REFERENSI

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