MODIFIKASI VIGENERE CIPHER DENGAN MENGGUNAKAN NILAI POSISI KARAKTER PADA TEKS

Irfan Afif (13507099)

Mahasiswa Program Studi Teknik Informatika
Institut Tenologi Bandung
Jl. Ganesha no. 10, Bandung
e-mail: irfan_afif@yahoo.com

ABSTRAK

Vigenere cipher merupakan salah satu algoritma enkripsi untuk menyembunyikan isi pesan dengan menggunakan kunci. Teknik enkripsi dari vigenere cipher adalah subtitusi setiap karakter pada teks menjadi karakter lain berdasarkan kunci yang diberikan. Jika panjang kunci lebih pendek daripada panjang teks, maka akan dilakukan perulangan pada kunci sehingga kunci yang nantinya digunakan akan memiliki panjang yang sama seperti panjang teks. Subtitusi karakter yang terjadi pada vigenere cipher bukanlah subtitusi tunggal seperti caesar cipher, tetapi subtitusi yang terjadi adalah subtitusi jamak. Hal ini dikarenaan dua huruf yang sama dapat di enkripsi menjadi 2 huruf yang berbeda.

Saat ini telah ditemukan suatu metode yang dapat menyerang Vigenere cipher dengan ampuh. Metode ini disebut dengan metode kasiski. Metode ini memanfaatkan pengulangan kunci pada vigenere cipher. Perulangan kunci dapat mengakibatkan hasil enkripsi yang sama untuk kata yang sama. Dengan mencari pola yang berulang ini nantinya kita dapat mencari kunci yang digunakan.

Dalam makalah ini penulis akan menuangkan idenya untuk memodifikasi vigenere cipher sehingga menjadi lebih kuat dan kebal terhadap metode kasiski. Ide penulis dalam memodifikasi vigenere cipher adalah dengan menggunakan posisi karakter pada teks. Penggunaan posisi karakter dapat menghilangkan pola berulang pada *cipher text*. Hal ini dikarenakan niai dari posisi karakter selalu berbeda. Dengan modifikasi ini diharapkan *cipher text* yang dihasilkan lebih kuat dan kebal terhadap serangan dari metode kasiski.

Kata kunci: Vigenere cipher, metode kasiski, posisi karakter.

1. PENDAHULUAN

Informasi merupakan hal yang sangat penting. Sejak zaman dahulu hingga sekarang, orang-orang terus melakukan usaha untuk menjaga informasi agar hanya orang-orang tertentu saja yang dapat mengetahui informasi terebut. Salah satu cara untuk melindungi informasi adalah dengan penyandian kata. Cabang ilmu yang mendalami penyandian kata ini disebut sebagai kriptografi.

Kriptografi telah digunakan dan dipelajari dari zaman dahulu. Bangsa mesir kuno telah menggunakan kriptografi sejak 4000 tahun silam. Dari dahulu hingga sekarang, telah bayak ditemukan algoritma-algoritma yang digunakan untuk menyembunyikan makna suatu pesan. Algoritma-algoritma tersebut saat ini dikenal memiliki dua pengelompokkan, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik biasanya adalah algoritma penyembunyian teks yang berorientasi pada huruf dan dapat dilakukan tanpa menggunakan komputer. Kriptografi klasik relatif lebih sederhana dibanding dengan kriptografi modern. Contoh dari kriptografi klasik adalah Caesar cipher dan Vigenere cipher. Kriptografi modern adalah algoritma yang memodifikasi teks secara bit. Hal ini dapat dilakukan karena pada zaman sekarang, informasi kebanyakan disimpan dan dikirim dengan menggunakan komputer. Di dalam komputer, informasi disimpan dalam bentuk bit sehingga hal ini mendasari lahirnya algoritma modern. Beberapa contoh dari kriptografi modern adalah DES dan AES.

2. LANDASAN TEORI

2.1 Vigenere Cipher

Vigenere cipher adalah suatu metode kriptografi yang digunakan untuk mengenkripsi suatu *plain text* menjadi *cipher text*. Nama Vigenere diambil dari seorang yang bernama Blaise de Vigenere. Blaise de Vigenere merupakan penemu dari Vigenere cipher. Walaupun begitu, ide dasar dari Vigenere cipher ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifradel. Sig. Giovan Battista Bellaso pada tahun 1553.

Gambar 1. Blaise de Vigenere

Vigenere cipher menggunakan teknik subtitusi. Teknik subtitusi yang digunakan mirip dengan teknik subtitusi Caesar cipher. Pada Caesar cipher, huruf pada *plain text* di enkripsi dengan cara menggesernya sejauh n pada deret alphabet. Hal ini dilakukan pada setiap huruf pada *plain text*. Hal ini mengekibatkan setiap huruf akan di enkripsikan menjadi huruf lain. Perubahan yang terjadi untuk setiap huruf yang sama adalah sama. Sebagai contoh saya memiliki *plain text*:

KRIPTOGRAFI MENYENANGKAN

Plain text di atas akan dienkripsi menggunakan Caesar cipher dengan n = 5 menjadi:

PWNUYTLWFKN RJSDJSFSLPFS

Dari *cipher text* dapat dilihat bahwa huruf I di enkripsi menjadi huruf N, huruf K menjadi huruf P dan seterusnya. Caesar cipher merupakan algoritma subtitusi tunggal dimana suatu huruf dienkripsi menjadi suatu huruf yang lain.

Vigenere cipher menggunakan teknik yang berbeda dengan Caesar cipher. Perbedaan mendasar antara Vigenere cipher dan Caesar cipher adalah penggunaan kunci untuk menentukan jumlah penggeseran pada huruf. Dengan memanfaatkan kunci, huruf yang sama pada *plain text* belum tentu di enkripsi menjadi huruf yang sama pada *cipher text*. Jika panjang kunci lebih pendek, maka akan dibentuk kunci baru yang terbentuk dari kunci lama yang diulang secara periodik. Pengulangan dilakukan sampai panjang kunci sama seperti panjang *plain text*. Jika kita memiliki *plain text* sebagai berikut:

INFORMATIKAITB

Kunci yang digunakan adalah:

HMIF

Cara pengenkripsiannya adalah:

Plain text	: INFORMATIKA ITB
Kunci	: HMIFHMIFHMI FHM
Cipher text	: PZNTYYIYPWI NAN

Algoritma enkripsi yang digunakan adalah dengan menggeser *plain text* sesuai kunci yang lokasinya bersesuaian. Pergeseran dilakukan dengan menggunakan table Vigenere. Walaupun begitu, pergeseran dilakukan dengan mengkonversi huruf menjadi angka dengan A=0 dan Z=25. Nilai n kunci yang digunakan pada makalah ini adalah nilai kunci. Hasilnya adalah huruf I pertama dienkripsi menjadi huruf P dan huruf I ketiga menjadi N. Dengan cara seperti ini Vigenere cipher dapat melakukan enkripsi subtitusi jamak.

	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 2. Tabel Vigenere Cipher

2.2 Metode Kasiski

Metode kasiski adalah metode yang dapat digunakan untuk menyerang *polyalphabetic subtitusion cipher*. Metode ini pertama kali dicetuskan oleh Friedreich Kasiski pada tahun 1863. Ide Kasiski adalah menentukan panjang kunci yang digunakan dengan menganalisis perulangan huruf yang terdapat dalam *cipher text*. Hal yang mendasari metode Kasaski adalah pada suatu bahasa terdapat pola huruf yang terdiri dari dua huruf atau lebih yang sering berulang. Sebagai contoh, pada bahasa Inggris pola huruf yang sering berulang adalah 'THE'.

Pada suatu teks, ada kemungkinan pola huruf yang sama di enkripsi oleh kunci yang sama. Hal ini di sebabkan oleh penggunaan kunci yang berulang. Besar kemungkinan pada *cipher text* akan terjadi pengulangan pola yang merupakan hasil enkripsi dari pola huruf yang sama pada *plain text*. Pola huruf ini kemungkinan besar dapat terjadi jika posisinya pada teks merupakan kelipatan dari panjang kunci. Dengan mencari faktor pembagi yang paling banyak dari posisi pola yang berulang pada *cipher text*, kita dapat menentukan panjang kunci vigenere cipher. Langkah-langkah metode Kasiski untuk menentukan panjang kunci adalah sebagai berikut :

1. Temukan semua pola huruf yang berulang.
2. Hitung posisi pola yang berulang pada *cipher text*.
3. Hitung semua faktor pembagi dari posisi pola yang berulang.
4. Faktor yang paling sering muncul kemungkinan besar adalah panjang kunci.

Contoh penerapan metode kasiski adalah:

Plain text	:BUKUDITARUHDIRAKBUKU
Kunci	:ABCDABCDABCDABCDABCD
Cipher text	: BVMXDJVDRVJGISCNBVMX

Pada *cipher text* ada satu pola yang berulang, yaitu BVMX. Jika ditelusuri, posisi pola yang berulang adalah di posisi 0 dan 16. Karena 0 tidak memiliki faktor, maka hanya nilai 16 yang akan dimanfaatkan. Faktor dari 16 adalah 2, 4, 8, dan 16. Karena panjang pola adalah 4, maka minimal panjang kunci adalah 4. Dengan begitu kita dapat memperkecil pilihan panjang kunci menjadi 4, 8 dan 16. Semakin panjang *plain text*, maka akan semakin banyak pula pola yang berulang dan panjang kunci akan lebih mudah ditemukan.

Setelah panjang kunci diketahui, kita memisahkan *cipher text* berdasarkan panjang kunci. Misalkan panjang kunci adalah 8. Langkah selanjutnya adalah memisahkan huruf-huruf pada *cipher text* menjadi kelompok huruf pertama, kelompok huruf kedua, kelompok huruf ketiga dan seterusnya. Dengan cara ini, *cipher text* telah dikelompokkan menjadi huruf-huruf yang dienkripsi dengan cara subtitusi tunggal. Oleh karena itu, masing-masing kelompok huruf ini dapat di serang dengan menggunakan metode analisis frekuensi.

3. MODIFIKASI VIGENERE CIPHER DENGAN MENGGUNAKAN NILAI POSISI KARAKTER PADA TEKS

Sebelum metode kasaiski ditemukan, Vigenere cipher dianggap sebagai algoritma enkripsi yang tidak dapat dipecahkan. Walaupun pada saat ini Vigenere cipher sangat rentan diserang dengan menggunakan metode kasiski, tetapi pada dasarnya Vigenere cipher adalah metode yang cukup kuat dan sederhana. Kesederhanaan dari Vigenere cipher ini memungkinkan modifikasi terhadap algoritma ini.

Kelemahan Vigenere cipher tercipta jika panjang kunci lebih pendek dari panjang *plain text*. Agar dapat mengenkripsi *plain text*, dibuatlah kunci baru yang diciptakan dari pengulangan kunci lama secara periodik. Hal ini memungkinkan terjadinya suatu pola huruf pada *plain text* dienkripsi dengan kunci yang sama sehingga mengakibatkan perulangan pola pada *cipher text*. Celah inilah yang digunakan oleh metode kasiski untuk menyerang Vigenere cipher.

Kelemahan Vigenere cipher tersebut sebenarnya dapat diatasi dengan menggunakan kunci yang panjangnya sama dengan panjang *plain text*. Tetapi hal ini menjadi masalah jika *plain text* memiliki nilai panjang yang besar. Plain text yang panjang membutuhkan panjang kunci yang panjang pula. Kunci yang sangat panjang menjadikan Vigenere cipher tidak efektif, karena teks yang panjang tidak praktis dan sulit diingat. Kunci yang sangat panjang menghilangkan kesederhanaan dari Vigenere cipher. Oleh karena itu cara seperti ini tidak dijadikan sebagai solusi untuk memperkuat Vigenere cipher.

Banyak ide-ide modifikasi yang telah dituangkan dalam makalah lain untuk memperkuat Vigenere cipher,

beberapa diantaranya adalah dengan menggunakan teknik subtitusi berulang pada kunci ataupun dengan cara menciptakan kunci baru yang unik dari kunci lama yang jumlahnya lebih dari satu. Inti dari modifikasi ini adalah menghasilkan kunci baru yang panjangnya sama dengan *plain text*, dihasilkan dari kunci yang sederhana serta bersifat acak Penulis memiliki suatu ide untuk memodifikasi Vigenere cipher. Ide modifikasi penulis adalah memanfaatkan nilai posisi karakter pada teks. Hal ini dikarenakan keunikan nilai posisi pada setiap huruf. Ada beberapa cara dalam memanfaatkan nilai ini, yaitu:

1. Jumlah pergeseran merupakan penjumlahan antara kunci dengan nilai posisi.
2. Jumlah pergeseran merupakan perkalian antara kunci dengan posisi.
3. Jumlah pergeseran merupakan kunci dipangkatkan nilai posisi.

3.1 Jumlah Pergeseran Merupakan Penjumlahan Antara Kunci dengan Nilai Posisi

Modifikasi Vigenere cipher dengan modifikasi penggeseran sebanyak penjumlahan antara kunci dengan nilai posisi Berikut adalah contoh penerapan modifikasi ini:

Plain text :
ALONGTIMEAGOACHILDWASBORNTOAQUEENA
NDKINGANDSHEWASCALLEDSNOWWHITEWHEN
THEQUEENDIEDTHEKINGMARRIEDAGAINTHISN
EWQUEENWASWICKEDANDHATEDSNOWWHITET
HEQUEENGAVEORDERSTHATSNOWWHITEWAST
OBETREATEDASASERVANTSNOWWHITEGREWV
ERYBEAUTIFULANDONEDAYAPRINCERIDINGBY
SAWHERATWORKANDFELLINLOVEWITHHERTHE
QUEENWASBEAUTIFULTOOANDEVERYDAYSHEA
SKEDHERMAGICMIRRORWHOISTHEFAIRESTINT
HELANDANDTHEMIRRORALWAYSANSWEREDYO
UARETHEFAIRESTONEOFALLBUTONEDAYTHEMI
RRORANSWEREDSNOWWHITEWASTHEFAIRESTI
NTHELANDANDINARAGETHEQUEENGAVEORDE
RSTOONEOFHERHUNTSMENTOTAKESNOWWHIT
EINTOTHEWOODSANDKILLHER

Kunci : HMIF

Kunci baru :
HNKILROMPVSQTZWUXDAYBHECFLIGJPMKNTQ
ORXUSVBYWZFCADJGEHNKILROMPVSQTZWUX
DAYBHECFLIGJPMKNTQORXUSVBYWZFCADJGE
HNKILROMPVSQTZWUXDAYBHECFLIGJPMKNTQ
ORXUSVBYWZFCADJGEHNKILROMPVSQTZWUX
DAYBHECFLIGJPMKNTQORXUSVBYWZFCADJGE
HNKILROMPVSQTZWUXDAYBHECFLIGJPMKNTQ
ORXUSVBYWZFCADJGEHNKILROMPVSQTZWUX
DAYBHECFLIGJPMKNTQORXUSVBYWZFCADJGE
HNKILROMPVSQTZWUXDAYBHECFLIGJPMKNTQ
ORXUSVBYWZFCADJGEHNKILROMPVSQTZWUX
DAYBHECFLIGJPMKNTQORXUSVBYWZFCADJGE
HNKILROMPVSQTZWUXDAYBHECFLIGJPMKNTQ
ORXUSVBYWZFCADJGEHNKILROMPVSQTZWUX
DAYBHECFLIGJPMKNTQORXUSVBYWZFCADJGE
HNKILROMPVSQTZWUXDAYBHEC

Cipher text:
HYYVRKWYTVYETBDCIGWYTISTSEWGZJQOATD
RBFHYVOBOGJYAVLGPSRNAYFKIWDLUPGAHQK
EOVLIPITMJCWQUVGWAROLAZEYCZNPTKRYRL
JACPVBIPNOYVJAXXQDFBAIFXYWCFWUDRMXS
HRYWIHYRDTTDHAYXONDAYFKIWDLUPZONLE
ERSLEVJOIYJHQBITDHJKIORIGPDLTEZEKVFOOIF
KWRJGSDWNJYADYYQYMPHPZOMXZQORIONEY
JVUUKQPCNGOKPSVXTZMSIXOZXXQPBBTUCFU
ACXMMGDIUPHEJCFXHVZWCNXICYVQKEZXOLS
VFYPBASFHNLLUWFPPWVMPNGRGQCGBDHYBF
SIEYJCYJEPRXVVEKTHRMEPIKMXQAXVRUYSLX
JJQIOATEDBGUCWXFDWVRKMJFABCNITVBZZIO
ZHRWHXCOHLZWFJAIYFDBNNUMSEXIHZKNZZM
YJCFPDLWGVHTOBSVEGTZFWTUAIOGEPTASQSP
WLQTDRHGJGDBHLJUYGDXPOZFNMARSVEFHTT
RGEWRWHANIJMOIT

Secara sekilas, kunci yang dihasilkan dari modifikasi ini menghasilkan kunci baru yang acak. Walaupun begitu, modifikasi ini memiliki kelemahan, yaitu menggunakan penjumlahan yang mudah untuk di runut balik. Dengan mengurangi (menggeser ke arah berlawanan) setiap karakter di *cipher text* sejumlah nilai posisinya, kita mendapatkan sebuah *cipher text* hasil Vigenere cipher tanpa modifikasi. *Cipher text* yang baru ini dapat diserang dengan menggunakan metode kasiski. Modifikasi seperti ini dirasa kurang efektif untuk memperkuat Vigenere cipher.

3.2 Jumlah Pergeseran Merupakan Perkalian Antara Kunci dengan Nilai Posisi

Modifikasi kedua adalah jumlah pergseran merupakan hasil kali antara kunci dengan nilai posisi karakter pada *plain text*. Dengan cara seperti ini, diharapkan kelemahan dari modifikasi yang pertama dapat dihilangkan. Hal ini dikarenakan suatu perkalian mudah dilakukan, tetapi sulit untuk menemukan faktor dari perkalian tersebut.

Dengan perkalian ini, walaupun salah satu nilai perkalian diketahui, untuk menentukan nilai dari kunci sangatlah sulit. Hal ini dikarenakan nilai hasil perkalian dijumlah terlebih dahulu dan menghasilkan suatu nilai. Kemudian dilakukan operasi mod kepada hasil penjumlahan tersebut. Melakukan perkalian, penjumlahan dan operasi mod tadi mudah dan sederhana jika kita mengetahui nilai *plain text* dan kunci untu menghasilkan nilai *cipher text*, tetapi sangat sulit untuk mencari nilai *plain text* dan kunci dari nilai *cipher text* yang diketahui.

Contoh penerapan modifikasi ini adalah:
Plain text :
ALONGTIMEAGOACHILDWASBORNTOAQUEENA
NDKINGANDSHEWASCALLEDSNOWWHITEWHEN
THEQUEENDIEDTHEKINGMARRIEDAGAINTHISN
EWQUEENWASWICKEDANDHATEDSNOWWHITET
HEQUEENGAVEORDERSTHATSNOWWHITEWAST
OBETREATEDASASERVANTSNOWWHITEGREWV
ERYBEAUTIFULANDONEDAYAPRINCERIDINGBY
SAWHERATWORKANDFELLINLOVEWITHHERTHE
QUEENWASBEAUTIFULTOOANDEVERYDAYSHEA
SKEDHERMAGICMIRRORWHOISTHEFAIRESTINT
HELANDANDTHEMIRRORALWAYSANSWEREDYO
UARETHEFAIRESTONEOFALLBUTONEDAYTHEMI
RRORANSWEREDSNOWWHITEWASTHEFAIRESTI
NTHELANDANDINARAGETHEQUEENGAVEORDE
RSTOONEOFHERHUNTSMENTOTAKESNOWWHIT
EINTOTHEWOODSANDKILLHER

Kunci : HMIF

Kunci baru :
AMQPCIWJEECDGAIXIWORKSULMOAFOKGZQG
MTSCSNUYYHWUEBYQKVAMQPCIWJEECDGAIXI
WORKSULMOAFOKGZQGMTSCSNUYYHWUEBYQ
KVAMQPCIWJEECDGAIXIWORKSULMOAFOKGZQ
GMTSCSNUYYHWUEBYQKVAMQPCIWJEECDGAI
XIWORKSULMOAFOKGZQGMTSCSNUYYHWUEB
YQKVAMQPCIWJEECDGAIXIWORKSULMOAFOK
GZQGMTSCSNUYYHWUEBYQKVAMQPCIWJEECD
GAIXIWORKSULMOAFOKGZQGMTSCSNUYYHWU
EBYQKVAMQPCIWJEECDGAIXIWORKSULMOAFO
KGZQGMTSCSNUYYHWUEBYQKVAMQPCIWJEEC
DGAIXIWORKSULMOAFOKGZQGMTSCSNUYYHW
UEBYQKVAMQPCIWJEECDGAIXIWORKSULMOAF
OKGZQGMTSCSNUYYHWUEBYQKVAMQPCIWJEE
CDGAIXIWORKSULMOAFOKGZQGMTSCSNUYYH
WUEBYQKVAMQPCIWJEECDGAIXIWORKSUL

Cipher text:
AXECIBEVIEIRGCPFTZKRCTICZHOFEEKDDGZWC
KFTULBZDYABQSKGLQTHPWSFLMVHCHMKBDS
HEWYYPWEIHRKJYTSFSTJVYBYNWCRUFYCIEIG
JGMJFEWYLIKMAIJRYKLYOEBOBKROSUZTXIW
WRHEYCAIVECHCOHMJHPWSFLMVHCAAQWXS
KBWUEQRAXOCKQLGZMKPGJQFGAAAVFULOM
YNUPWBEOYPCQJOVBLWMRZJCYOSRNRSTFREE
TOJWEURUVNEEOBVOGLUDAQDAFMXJKKRBEM
MIVOFQLEPEFIDOEKRFHGCFQYTCYUXEZQXOVS
WUSJMNVEKKFSIZOWNKYYAMETSFFWBKRJOZ
MZGDNHBYUZNLFKYBMODQAYIUBERUZKRMA
GKIRBWNSQTANFOYSETQHXCDYVSRVJYHBWJR
ZMUHGQZWWWAGUKDAKWSKYSLYHMGTMSPG
HHKEMAPLUYJYUZUREGDKMASUIJMMDIIPJGV
MLZZSICLIZZSOKVOXGKTFLEGFGIRYRAMRPUM
RDTQYCVWPQIAQRJSIKLGWCVZYC

Kelemahan dari modifikasi ini adalah huruf pertama dari *plain text* tidak berubah. Hal ini dikarenakan posisi awal dianggap memiliki nilai nol. Bilangan apapun dikalikan dengan nol akan mengasilkan nol. Sedangkan bilangan apapun jika ditambah dengan nol akan menghasilkan bilangan itu sendiri. Oleh karena itu huruf pertama pada *plain text* sama dengan huruf pertama pada *cipher text*. Hal ini mungkin dapat menyebabkan terbongkarnya *cipher text* walaupun hanya satu huruf yang terdecipher. Walaupun begitu kelemahan ini dapat dengan mudah ditutup dengan menggeser nilai posisi karakter sebanyak satu atau lebih.
.

3.3 Jumlah Pergeseran Merupakan Hasil Perpangkatan antara Kunci dengan Posisi Karakter

Modifikasi yang ketiga menggeser huruf sejauh kunci dipangkatkan dengan posisi karakter. Berikut adalah contoh penerapan modifikasi dengan pangkat:

Plain text :
ALONGTIMEAGOACHILDWASBORNTOAQUEENA
NDKINGANDSHEWASCALLEDSNOWWHITEWHEN
THEQUEENDIEDTHEKINGMARRIEDAGAINTHISN
EWQUEENWASWICKEDANDHATEDSNOWWHITET
HEQUEENGAVEORDERSTHATSNOWWHITEWAST
OBETREATEDASASERVANTSNOWWHITEGREWV
ERYBEAUTIFULANDONEDAYAPRINCERIDINGBY
SAWHERATWORKANDFELLINLOVEWITHHERTHE
QUEENWASBEAUTIFULTOOANDEVERYDAYSHEA
SKEDHERMAGICMIRRORWHOISTHEFAIRESTINT
HELANDANDTHEMIRRORALWAYSANSWEREDYO
UARETHEFAIRESTONEOFALLBUTONEDAYTHEMI
RRORANSWEREDSNOWWHITEWASTHEFAIRESTI
NTHELANDANDINARAGETHEQUEENGAVEORDE
RSTOONEOFHERHUNTSMENTOTAKESNOWWHIT
EINTOTHEWOODSANDKILLHER

Kunci : HMIF

Kunci baru:
BMMVJMMVDXMVXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X

Ketika dilakukan pengetesan dengan komputer yang saya miliki, hasil yang keluar seperti di atas. Hal ini disebabkan karena hasil komputasi yang dihasikan sangatlah besar. Misalkan saja nilai kunci adalah 20 dan berada pada posisi 300, hal ini tentu menghasilkan angka yang sangat besar. Walaupun tingkat kerumitan dari pangkat adalah yang paling besar dari ketiga modifikasi ini, tetapi modifikasi ini membutuhkan resource computer yang cukup besar untuk dapat melakukan komputasi perpangkatan yang besar. Selain itu juga kelemahannya adalah kunci baru yang terbentuk pasti diawali dengan huruf B. Tetapi hal ini dapat diatasi dengan cara yang sama seperti pada pekalian.

4. Kesimpulan

Berdasarkan analisis dan pengujian modifikasi Vigenere cipher dengan posisi karakter, penulis mendapatkan beberapa kesimpulan. Kesimpulan tersebut adalah:

1. Posisi karakter pada *plain text* dapat digunakan untuk memperkuat Vigenere cipher, yaitu dengan cara menciptakan kunci baru yang memiliki panjang yang sama dengan *plain text* dan relatif bersifat acak.
2. Pembuatan kunci baru dengan metode pada kesimpulan satu dapat dilakukan dengan tiga cara, yaitu penjumlahan kunci dengan posisi, perkalian kunci dengan posisi dan perpangkatan kunci dengan posisi.
3. Pembuatan kunci baru dengan cara penjumlahan memiliki keunggulan sederhana dan mudah dilakukan. Sedangkan kelemahannya adalah mudah untuk membalik proses penjumlahan tersebut, sehingga *cipher text* tetap bisa diserang dengan metode kasaski.
4. Pembuatan kunci baru dengan cara perkalian dapat melindungi Vigenere cipher dari metode kasiski. Hal ini dikarenakan sifat perkalian, yaitu mudah untuk melakukan perkalian tetapi sulit untuk mencari faktor dari perkalian tersebut. Kelemahan cara ini adalah huruf pertama pada *plain text* dan *cipher text* sama. Walaupun penulis belum mengetahui cara untuk menafaatkan kelemahan ini, tetapi menurut penulis hal ini bisa menjadi ancaman nantinya. Kelemahan ini dapat diatasi dengan menggeser nilai posisi karakter sehingga di posisi awal bukan bernilai nol.
5. Pembuatan kunci baru dengan cara perpangkatan memiliki tingkat kerumitan tertinggi dibanding cara lainnya. Hal ini dikarenakan pangkat merupakan perkalian yang berulang. Walaupun begitu cara ini memiliki kelemahan, yaitu membutuhkan sumber daya yang besar untuk dapat melakukannya.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[2] http://www.braingle.com/brainteasers/codes/vigenere.php
Waktu akses: 26 Maret 2010 pukul 05.18