Teknik Kriptografi Block Cipher dengan VBR (Perputaran Bit Vertikal)

Hanson Prihantoro Putro (13505045)
Jurusan Teknik Informatika STEI ITB, Bandung 40135, email: if15045@students.if.itb.ac.id

Abstract *– Makalah ini membahas tentang salah satu algoritma kriptografi modern namun sederhana. Algoritma ini melakukan manipulasi terhadap nilai-nilai bit dari tiap karakter yang akan dienkripsi atau didekripsi. Perkembangan kriptografi kini adalah bagaimana orang berlomba-lomba membuat suatu teknik kriptografi yang serumit mungkin tanpa memperhatikan kesederhanaannya karena nantinya komputerlah yang melakukan perhitungan rumit ini. Namun dengan algoritma yang kami ajukan ini, diharapkan kesederhanaan logika pengenkripsian tetap bisa dipertahankan. Algoritma ini sesederhana algoritma kriptografi klasik namun dengan keamanan sekuat algoritma kriptografi modern. Untuk pengembangan selanjutnya, pada makalah akan disertakan tahap-tahap enkripsi secara lebih detail, penggunaan key, contoh kode enkripsi, contoh penggunaan serta analisis serangan yang mungkin bisa dilakukan ke ciphertext-nya. Diharapkan dengan pengembangan teknik kriptografi ini, akan menambah daftar teknik-teknik kriptografi yang sederhana namun luar biasa, yang berguna bagi lalu lintas komunikasi dan informasi yang membutuhkan keamanan dan kenyamanan.*

Kata Kunci*:kriptografi, ASCII, plaintext, ciphertext, key, enkripsi, dekripsi, .*

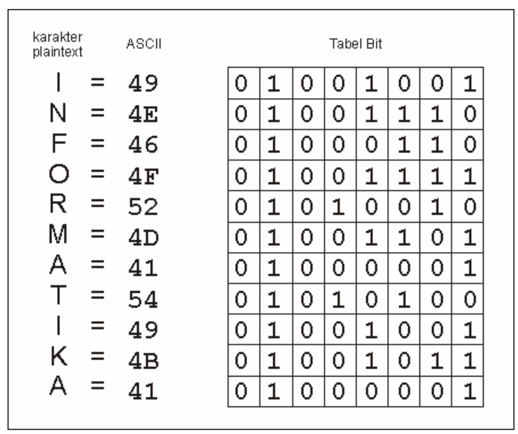
1. PENDAHULUAN

Dalam perkembangannya, banyak sekali teknik-teknik kriptografi yang dikembangkan untuk memperoleh hasil yang memuaskan. Setiap proses-proses enkripsinya dibuat sedemikian rumitnya hingga hasil *ciphertext*-nya tidak mudah dianalisis. Namun sebenarnya, jika kita bisa mengolah teknik kriptografi lama, kita mendapatkan teknik yang sederhana, namun tetap tidak mudah uuntuk dianalisis. Salah satunya adalah teknik Perputaran Bit Vertikal (Vertical Bit Rotation/VBR) teknik yang coba penulis kembangkan melalui makalah ini.

Pengambangan teknik VBR, terinspirasi oleh teknik kriptografi klasik yaitu teknik transformasi dan teknik kriptografi modern yaitu dengan pemanipulasian bit. Dengan memanfaatkan teknik klasik, kita mendapatkan kesederhanaan enkripsi, sedangkan dengan menambahkan teknik modern, kita bisa mempersulit para kriptanalasis yang mencoba membuka hasil enkripsi ini. Diharapkan dengan mengkolaborasikan kedua teknik tersebut, kita bisa mendapatkan keuntungan dari teknik-teknik tersebut dan menghilangkan kerugiaanya.

2. PENJELASAN KRIPTOGRAFI VBR

Berikut akan dijelaskan secara singkat bagaimana teknik VBR ini bekerja. Pertama-tama, setiap karakter dari teks yang akan dienkripsi ataupun didekripsi, nilai ASCII-nya diubah ke dalam bit. Sebagai salah satu kriptografi cipher blok, teknik ini akan memproses setiap blok-blok bit tersebut, dimana VBR akan lebih optimal jika pembagian dilakukan ke dalam 256 bytes. Kemudian,kita susun bit-bit tersebut secara vertikal berdasarkan karakter-karakter pembentuknya. Kini, kita telah mendapatkan sebuah ’tabel’ bit yang terdiri dari 8 kolom dan 256 baris.



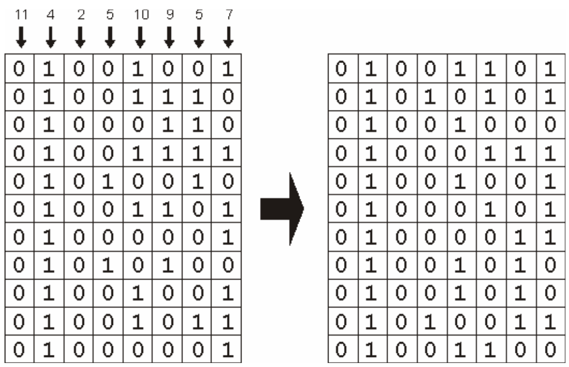
karakter plaintext		ASCII	Tabel Bit							
I	=	49	0	1	0	0	1	0	0	1
N	=	4E	0	1	0	0	1	1	1	0
F	=	46	0	1	0	0	0	1	1	0
O	=	4F	0	1	0	0	1	1	1	1
R	=	52	0	1	0	1	0	0	1	0
M	=	4D	0	1	0	0	1	1	0	1
A	=	41	0	1	0	0	0	0	0	1
T	=	54	0	1	0	1	0	1	0	0
I	=	49	0	1	0	0	1	0	0	1
K	=	4B	0	1	0	0	1	0	1	1
A	=	41	0	1	0	0	0	0	0	1

Gambar 1. Tahap awal sebelum enkripsi/dekripsi kriptografi VBR

2.1. Enkripsi

Kemudian dalam proses enkrirpsi, kita membutuhkan *key* untuk menyembunyikan nilai-nilai bit dari karakter yang terkorespondensi. Disini, nilai *key* digunakan untuk menggeser secara vertikal nilai-nilai bit yang ada. Karena kita memiliki 8 kolom untuk kita geser, kita memerlukan 8 bilangan penggeser. Sebagai percobaan, kita akan menggeser bit-bit pada gambar diatas. Kita ambil contoh dengan key berupa bilangan (11, 4, 2, 5, 10, 9, 5, 7). Dengan key tersebut, kita akan menggeser bit-bit pada kolom pertama sebanyak

11 baris ke bawah, pada kolom kedua sebanyak 4 baris ke bawah, begitu seterusnya hingga kolom kedelapan. Untuk contoh ini, dalam 1 blok kita tidak perlu menggunakan tepat 256 baris karena teknik ini lebih optimal dilakukan jika ada blok yang ukurannya kurang dari 256 bytes, tidak perlu ditambahi nol lagi (*padding*).



Gambar 2. Tahap utama enkripsi kriptografi VBR

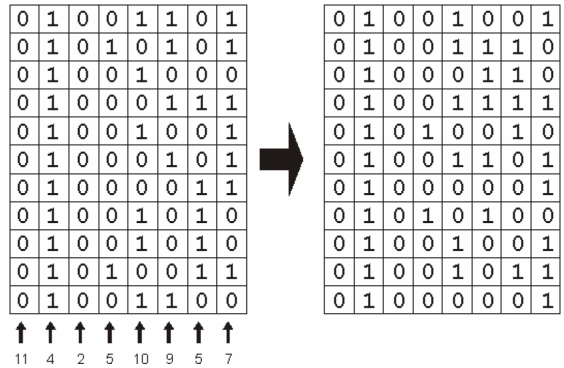
Setelah kita mendapatkan nilai pergeseran tersebut, maka kita telah medapatkan nilai-nilai bit yang kemudian berkorespondensi dengan karakter-karakter untuk *ciphertext*-nya. Pada contoh diatas, karakter-karakter pada kata "INFORMATIKA" yang dienkripsi dengan *key* (11, 4, 2, 5, 10, 9, 5, 7) akan menjadi karakter-karakter "MUHGIECJJSL".

Tabel Bit								ASCII		karakter ciphertext
0	1	0	0	1	1	0	1	4D	=	M
0	1	0	1	0	1	0	1	55	=	U
0	1	0	0	1	0	0	0	48	=	H
0	1	0	0	0	1	1	1	47	=	G
0	1	0	0	1	0	0	1	49	=	I
0	1	0	0	0	1	0	1	45	=	E
0	1	0	0	0	0	1	1	43	=	C
0	1	0	0	1	0	1	0	4A	=	J
0	1	0	0	1	0	1	0	4A	=	J
0	1	0	1	0	0	1	1	53	=	S
0	1	0	0	1	1	0	0	4C	=	L

Gambar 3. Hasil enkripsi kriptografi VBR

2.2. Dekripsi

Untuk proses dekripsinya, caranya tidak jauh berbeda. Jika pada proses enkripsi kita menggeser bit-bit ke bawah, untuk proses dekripsi, kita cukup menggeser bit-bit *ciphertext* ke atas sebanyak nilai-nilai *key* pada kolom yang bersesuaian.



Gambar 4. Tahap utama dekripsi kriptografi VBR

2.3 Penggunaan Kunci

Variasi kunci sebesar 64 bit (8 bilangan berukuran 1 bytes, untuk blok sebesar 256 bit). Ini berarati kita bisa menyediakan kunci, jika berupa kumpulan karakter, panjang maksimal 8 karakter. Hal ini karena setiap byte digunakan untuk menggeser tiap kolom blok. Sebenarnya penggeseran dilakukan dengan 8 bilangan, namun untuk kriptografi ini, kunci bisa disimpan dalam kumpulan karakter (kalimat) yang terdiri dari 8 karakter. Jika karakter kunci kurang dari 8 maka akan disisipi nilai 0 sebagai penggeser. Jika karakater lebih dari 8 maka karakter selainnya diabaikan.

3. HASIL DAN PEMBAHASAN

Berikut contoh kata yang akan dienkripsi:

"Inggris, Bagi Anda pengguna online banking HSBC, sebaiknya waspada. Para peneliti di Inggris telah memperingatkan nasabah HSBC, akan adanya kerentanan pada sistem online banking perusahaan tersebut. Dua peneliti yang bekerja pada Fakultas Ilmu Komputer Cardiff University, Professor Antonia J Jones serta Joseph R. Rabaiotti bersama dengan peneliti independen Stuart P Goring, berhasil menemukan kerentanan dalam sistem perbankan online situs HSBC. Tanpa menunjukkan kemampuan hacking atau mencoba memasuki sistem tersebut, ketiga peneliti ini hanya mendemokan kerentanan sistem tersebut menggunakan key logger. Key logger sendiri merupakan sebuah perangkat yang biasa digunakan para black hacker untuk merekam tombol yang ditekan konsumen online bankig, sehingga mereka dapat mengambil semua informasi penting konsumen. Ketiga peneliti tersebut, telah menginformasikan kepada pihak HSBC perihal kerentanan dalam situs mereka, sebelum didemontrasikan kepada khalayak ramai. Selama melakukan penelitian mereka juga mengklaim tidak pernah mencoba memasuki area terlarang, meskipun sebenarnya mereka sanggup. Lalu kenapa mereka tidak menyusupi sistem tersebut? Seperti dikatakan para peneliti tersebut yang dilansir Vnunet dan dikutip detikINET, Selasa (15/8/2006), poin yang paling penting adalah mereka berhasil menemukan dan mengidentifikasi celah yang dapat digunakan untuk mengambil informasi penting konsumen."

Dan hasil dekripsinya adalah sebagai berikut:

"`a!kpkb``k$shBI bdil!bkctam&ezdita
b`da2ibag=d{}nmh$e`ajlk(ee`cf`e2iqsx
gcdfba4aw|olx}`'$
  ^DO<anajazee0al`g)a``q`da2ghbm'ebR
iylud)inUc%deX{tetiahGs`pl!!kdGb"clF
e4oech}loh$e`ajnk(gehcb`i&q`FA
 ioc`agrca1fyva`bb!0a~Do<alabmphk$ed
)c`Aulti0idlgc'jivepmaheyd`p|f9i&MvA
`dj!
hygkvlgo$mcigy`fam$exfitafhfi&ak`ce=
fqsd`a8lqhginlmh$e`kbeg2isprk,}jM@
$ HE^go.anxciuk`lei%cejgyrbhk)ge`ad
ad)wlui&cajglea!eaapso"fu@llad7`iRm{
tarzd$7pkEcsxd}l,arKchjn&g
AcDsg0hyv`g+cpJtb`2`) ggO``qtbc(gqse
lfe(eablfo<alahivgd"mde~da`de`1wp@FV
G%cc`nuo2hahevcg
kp{uc`dce8aard`i6mragibhue0i`ba#copd
m%ib{ec``ba0itbh#ic`ja%acldwl0kwtam"
kucmlfi=fi`hge2m`dm"iwkhlea.gmuylloh
&ebcjni
mgajja!;`ag=fsuf`a6cu|ghrtm!$aqcndo<
alaji|aj!hla"ie|ee,loaieibdam$ezditc
j`ce?dsuf`a6awtkd~ue$meib{ek`lai-
fvg%kmnh h#,!
      uibfac&crihbi2ic`ba
qdHI Itibdao&gxdivadhdi&ak`ge0kuvqm
iua`fa-
4odamrdo,meg`bhyqiui`daa&cxk`kd+`kac
qhdi9mohm`!,%
 CIElek
oakgq`ldm<alahgyfdoi)dgdaiedao
aqe``c&ktlue*ekida`lee1iivod(g`iqca|
dm8dgzknea.em}ujlho*!&/ AQAnfm<clcb
et`c4au|g`t|d)0idngm*emdhe`iyaihgtcm
aqmbdk0ielma&agyqpypag=dqwd`c4au|g`s
tq%0mpB xba%k`kua`b`a0a|fm<anabet`c4
autk`xue0mhdk&ibaa|d|f7dqDhtc.hbe/c`
std|i(kuelg``\E aiArlo)50-
2!9afda)ulgm*gijeao`fi0aafjg8`ydlei$
achelgc!miaqsbgb!udhe0byfmtifdi)!a d
artco4ahmbbyetcm"asajeg6eimlx h'($
CNWa
cl0iu~eg(gikdijdmf(e`ksaa~dm8dgzknea
.em}}n`ab",: :,(%;bhgg0ajli4ebandm8
fgpadid+biddcm csadha
hyeitneo$mcigqdjdi$leo
emfmblipciaac~ei
k`hge2eb`a&a|`tm%ib{ealde"

Dari plaintext, huruf-huruf yang sering muncul adalah 'A', 'E', kemudian 'N'. Walaupun pada ciphertext huruf yang paling banyak muncul adalah 'A', 'E', dan 'D', namun setiap huruf 'A' pada ciphertext tidak berasosiasi dengan huruf 'A' pada plaintext. Oleh karena itu, algoritma ini tidak dapat dipecahakan dengan teknik analisis frekuensi.

Algoritma ini dapat menyediakan variasi kunci sebesar 64 bit / 8Bytes. Tidak banyak komputer yang mampu melakukan exhaustive search kurang dari 1 tahun untuk mencari kemungkinan yang cocok dari kombinasi karakter untuk mendapatkan kuncinya.

4. KESIMPULAN

Algoritma kriptografi Perputaran Bit Vertikal (Vertical Bits Rotation / VBR) cukup aman digunakan sebagai mudal dari kotak enkripsi/dekripsi pada blok cipher. Dengan algoritma dan pembuatan yang sederhana, algoritma ini memberikan keamanan yang bisa diandalkan.

DAFTAR REFERENSI

[1] Munir, Rinaldi, "*Diktat Kuliah IF5054 Kriptografi*", ITB, Bandung, 2005
[2] Bellare, Mihir, "*Introduction to Modern Cryptography*", Universisty of California, California, USA, 2005
[3] A. Menezes, "*Handbook of Applied Cryptography*", CRC Press, 1996