Penerapan Algoritma Vertical Bit Rotation (VBR) Dalam Penyimpanan File Online

Ebiet Nico Citra
STMIK Budi Darma Medan, Jl. SM.Raja No.338 Sp.Limun Medan, Sumut, Indonesia.
// E-mail : ebietnicocitra@gmail.com

ABSTRACT
Many facilities offered, but in terms of security, there is no absolute security. One way to secure files is to encrypt the file with cryptographic algorithms, and in this study Vertical Bit Rotation (VBR) cryptographic algorithms will be used as cryptographic algorithms that are used to increase the level of security in terms of storing files online. This algorithm is as simple as the classic cryptographic algorithm but with the security as strong as modern cryptographic algorithms. For further development, the paper will include stages of encryption in more detail, use of keys, examples of encryption codes, and examples of usage.

Kata Kunci : Kriptografi, Vertical Bit Rotation

PENDAHULUAN

Seiring berkembangnya teknologi *internet*, teknologi *website*, sebagai *interface* yang menjembatani antara pengguna dan dunia maya, juga ikut berkembang [3]. Berbagai macam bahasa pemrograman *web* digunakan, dan semakin lama semakin disempurnakan mengikuti perkembangan teknologi-teknologi yang berkaitan. *Web design* juga tak kalah berkembangnya, menjadikan dunia maya lebih menarik [6]. Penggunaan aplikasi berbasis *web* sedang popular pada saat ini, karena perancangan, pembangunan, dan pengimplementasian serta penggunaan aplikasi berbasis *web* dirasa lebih mudah. Juga tergolong lebih mudah dalam hal perubahan dan pengembangan.

Penyimpanan *file* secara *online* sudah banyak dilakukan. Teknik ini mempermudah proses pengaksesan data karena tidak dibatasi kapan dan dimana kita membutuhkan *file* tersebut. Tidak lagi memerlukan tempat menyimpan data dengan kapasitas besar yang harus dibawa kemana-mana. Hanya memerlukan koneksi *internet* dan langsung dapat mengakses *file* yang diinginkan, kapan saja, dimana saja. Telah banyak situs-situs yang menawarkan jasa penyimpanan data secara *online,* baik yang berbayar maupun yang gratis. Namun untuk yang gratis biasanya mendapatkan fasilitas yang lebih terbatas. Contoh-contoh dari penyimpanan *fileonline* yaitu *Rapidshare, Megaupload, Hotfile, Filesonic, Duckload, Wupload, Uploaded, Extabit, FileServe, Mediafire, Jiddu, 4shared, Indowebster, Enterupload* dan lain-lain.

LANDASAN TEORI

Kriptografi bertujuan untuk memberikan layanan pada aspek-aspek keamanan [5] antara lain :

1. Kerahasiaan (*confidentiality*), yaitu menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*), yaitu memberikan jaminan bahwa untuk tiap bagian pesan tidak akan mengalami perubahan dari saat datadibuat/dikirim oleh pengirim sampai dengan saat data tersebut dibuka oleh penerima data.
3. Otentikasi (*authentication*), yaitu berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan,
4. Nirpenyangkalan (*non repudiation*), yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang tertentu sehingga apabila ada seseorang yang mencoba mengakui memiliki dokumen tersebut, dapat dibuktikan kebenarannya dari pengakuan orang tersebut.

2.1. Kriptografi *Vertical Bit Rotation* (VBR)

Salah satu hal yang penting dalam komunikasi menggunakan komputer untuk menjamin kerahasiaan data adalah enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang biasa dimengerti menjadi sebuah kode yang tidak biasa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *chipper* [8]. Sebuah chipper menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti

(*unintelligible*). Karena teknik *chipper* merupakan suatu sistem yang telah siap untuk di automasi, maka teknik ini digunakan dalam sistem keamanan komputer dan *network*.

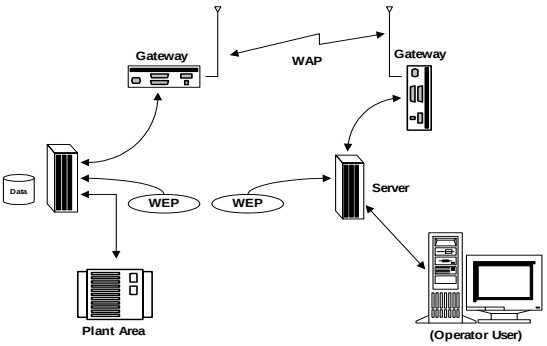
Kriptografi VBR sebagai salah satu *chipper* merupakan suatu *encryption* algoritma yang dikembangkan oleh *National Security Agency* Badan Keamanan Nasional Amerika Serikat (NSA) untuk *Clipper Chip.*Tidak banyak diketahui algoritma VBR ini, karena itu VBR digolongkan rahasia oleh pemerintah Amerika Serikat.

Algoritma VBR diketahui suatu algoritma *symmetric*, yang menggunakan 64-bit kunci dan mempunyai 32 putaran untuk memproses setiap masing-masing *encrypt* atau *decrypt* operasi. *Clipper-Chip* adalah suatu chip komersil dibuat oleh NSA untuk *encryption*, dan menggunakan Algoritma VBR. AT&T mempunyai rencana untuk menggunakan *Clipper Chip* untuk *encrypted* jalur suara telpon.

2.2. Keamanan Kriptografi Vertical Bit Rotation (VBR)

Sejauh yang diketahui, NSA tengah VBR ke *encrypt messaging* sistemnya, sehingga dirasakan algoritma itu aman. Kriptografi VBR menggunakan 64-bit kunci, yang berarti ada 2^64 (kira-kira 10^24) atau lebih dari 1 kunci mungkin trilyun untuk digunakan!! Maknanya, diperkirakan lebih dari 400 milyar tahun tiap-tiap kunci algoritma untuk dapat dipecahkan!

Untuk memberi suatu perspektif lebih baik, jika kita mengasumsikan penggunaan 100,000 RISC komputer, masing-masing dengan kemampuan menjalankan motor sekitar 100,000 *encryptions* per detik, akan diperkirakan sekitar 4 juta tahun suatu kode dapat dipatahkan. Pengembang Kriptografi VBR memperkirakan bahwa biaya daya proses untuk memecahkan algoritma kriptografi VBR dibagi dua untuk tiap-tiap delapan belas bulan, dan berdasarkan pada itu algoritma VBR akan membutuhkan sedikitnya 36 tahun baru dapat dipatahkan. Oleh karena itu, NSA percaya bahwa tidak ada resiko Kriptografi VBR dapat dirusakkan di dalam 30-40 tahun kedepan. Di samping itu, kekuatan Kriptografi VBR mampu melawan terhadap suatu serangan *cryptanalytic*. Untuk itu algoritma Kriptografi VBR harus mengarah kepada algoritma yang *cryptographic* dengan sepenuhnya ditetapkan dan digolongkan RAHASIA.



Gambar 1. Urutan proses pengiriman data
Sumber :
http://www.sumutweb.com/algoritma_vbr.pdf
tanggal akses 1 Mei 2011 jam 19.57 WIB

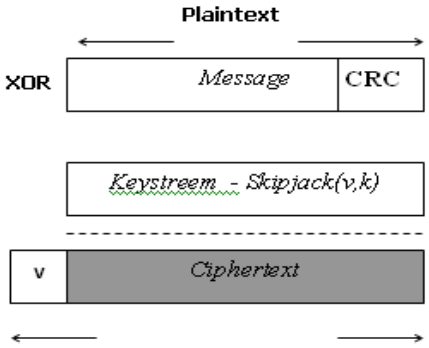
Algoritma yang *crytographic* mempunyai karakteristik seperti berikut:

1. *Symmetric*, algoritma 64-bit kunci *encryption/decryption*.
2. Berfungsi serupa dengan DES (yaitu., pada dasarnya suatu 64-bit kode membukukan perubahan bentuk yang dapat digunakan pada tempat yang sama dengan empat mode operasi ketika ditetapkan untuk DES di dalam FIPS 81).
3. Mampu memproses dengan 32 putaran *encrypt/decrypt* pada operasi tunggal.

Chip Clipper pada Algoritma kriptografi VBR berisi *single-key* 64-bit blok *encryption* algoritma. Algoritmanya menggunakan 64 kunci bit (bandingkan dengan DES hanya 56 kunci bit) dan mempunyai 32 putaran yang berebut (bandingkan dengan DES hanya 16 putaran), algoritma ini mendukung 4 mode operasi DES. Algoritma mengambil 32 *thick clock*, dan di dalam *Codebook Elektronik* (ECB) mode berjalan pada 12 Mbits per detik. Dengan penjelasan seperti diatas, Kriptografi VBR dapat dikatakan sangat dipercaya atau sangat menjamin.

2.3. Spesifikasi Algoritma Kriptografi *Vertical Bit Rotation* (VBR)

Standard spesifikasi penggunaan algoritma Kriptografi VBR di implementasikan pada peralatan elektronik (seperti chip elektronik dengan skala besar) peralatan elektronik tersebut mengandung modul *cryptograph* yang di integrasikan pada *product chip* telekomunikasi. Persetujuan implementasi telah di otorisasi Organizations for Integration into Security Equipment Peralatan tersebut harus di validasi oleh The National Institute of Standards and Technology (NIST) yaitu suatu Institut Teknologi Dan Standard Nasional Amerika Serikat dengan standard FIPS 140-1.



Gambar 4 Frame enkripsi
Sumber :
http://www.sumutweb.com/algoritma_vbr.pdf
tanggal akses 1 Mei 2011 jam 19.56 WIB

Spesifikasi algoritma Kriptografi VBR mempunyai ketentuan fungsi sebagai berikut :

1. Data *Encryption: Session key* harus menggunakan panjang *key* 64 bits untuk melakukan *encryption plaintext* dengan menggunakan mode operasi salah satu dari yang dispesifikasikan pada FIPS-81: ECB, CBC, OFB(64), CFB (1, 8, 16, 32, 64).
2. Data *Encryption: Session key* (64 bits) digunakan untuk *encrypt* data, juga digunakan sebagai *decrypt* hasil dari *ciphertext*.

PEMBAHASAN

Proses rotasi pada setiap kolom besarnya tergantung pada variabel rotasi (*r*). Proses ini membutuhkan variabel-variabel rotasi untuk merotasi kolom bit pada tabel bit sesuai dengan jumlah kolom pada tabel bit. Ukuran maksimal dari blok penyandian adalah 256. Angka ini dapat diwakili oleh karakter ASCII. Sehingga untuk mendapatkan variabel rotasi, bisa didapat dari nilai karakter ASCII yang dimasukkan melalui kunci.

Dari pemikiran ini maka dapat disimpulkan bahwa dibutuhkan karakter-karakter ASCII yang diambil nilai desimalnya untuk menjadi nilai dari variabel-variabel rotasi yang dibutuhkan. Jumlah kolom pada tabel bit adalah 8 kolom bit. Sehingga bila satu buah kolom membutuhkan satu buah nilai variabel rotasi, maka dibutuhkan 8 buah nilai variabel rotasi. Bila nilai variabel rotasi diambil dari nilai desimal masing-masing karakter pada kunci, maka dibutuhkan sebuah kunci dengan panjang 8 karakter.

Sedangkan variabel rotasi yang mengambil nilai desimal dari karakter ASCII kunci, tidak memiliki batasan tertentu. Sehingga rotasi dapat bernilai nol (0) ataupun sama dengan ukuran blok penyandian. Apabila kondisi ini terjadi, maka tidak akan terjadi rotasi bit atau rotasi terjadi namun bit kembali pada tempat semula, dan blok penyandian tidak terenkripsi.

3.1. Tidak Ada Perubahan Bit pada Algoritma Kriptografi *Vertical Bit Rotation*

Berikut akan dijelaskan secara singkat bagaimana teknik *Bit Vertical Bit Rotation* 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. Kemudian bit-bit tersebut susun secara vertikal berdasarkan karakter-karakter pembentuknya. Diambil contoh dari sebuah *file* yang bernama TES.doc dimana isi dari sebuah *file* tersebut adalah "NETTIMARINA".

Tabel 1 Tahap awal sebelum enkripsi/dekripsi kriptografi VBR

Karakter Plaintext	ASCII	Tabel Bit							
N	4E	0	1	0	0	1	1	1	0
E	45	0	1	0	0	0	1	0	1
T	54	0	1	0	1	0	1	0	0
T	54	0	1	0	1	0	1	0	0
I	49	0	1	0	0	1	0	0	1
M	4D	0	1	0	0	1	1	0	1
A	41	0	1	0	0	0	0	0	1
R	52	0	1	0	1	0	0	1	0
I	49	0	1	0	0	1	0	0	1
N	4E	0	1	0	0	1	1	1	0
A	41	0	1	0	0	0	0	0	1

3.2. Proses Enkripsi

Dalam proses enkrirpsi, proses 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, akan dilakukan penggeser bit-bit pada gambar diatas. Dan sebagai contoh diambil *key* berupa bilangan (11, 3, 10, 5, 2, 4, 5, 7). Dengan *key* tersebut, akan dilakukan penggeser bit-bit pada kolom sebanyak 11 baris ke bawah, pada kolom kedua sebanyak 4 baris ke bawah, begitu seterusnya hingga kolom kedelapan. Untuk contoh ini, dalam 1 blok 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.

Untuk Menjelaskan proses diatas dapat dilihat proses berikut ini :

1. Konversi Plainteks kebentuk *Binary*
2. *Set Binary* menjadi 8 bit (8 Karakter)

3. Tempatkan Kunci ke setiap *Bit Binary*, sehingga dihasilkan informasi *key* dan *binary* seperti tabel dibawah ini :

Tabel 2 Tahap awal untuk pembentukan kunci

Key	11	3	10	5	2	4	5	7
N = 4E	0	1	0	0	1	1	1	0
E = 45	0	1	0	0	0	1	0	1
T = 54	0	1	0	1	0	1	0	0
T = 54	0	1	0	1	0	1	0	0
I = 49	0	1	0	0	1	0	0	1
M = 4D	0	1	0	0	1	1	0	1
A = 41	0	1	0	0	0	0	0	1
R = 52	0	1	0	1	0	0	1	0
I = 49	0	1	0	0	1	0	0	1
N = 4E	0	1	0	0	1	1	1	0
A = 41	0	1	0	0	0	0	0	1

4. Lakukan putaran pada setiap kolom dari atas ke bawah sebanyak kunci yang di berikan
   a. Kolom 1 : di putar kearah bawah sebanyak 11 putaran

0	0	0	0	0	0	0	0	0	0	0

Karena Kolom 1 semua bernilai 0 maka ketika dilakukan perputaran sebanyak 11 kali akan tetap seperti nilai semula

0	0	0	0	0	0	0	0	0	0	0

   b. Kolom 2 : di putar kearah bawah sebanyak 3 putaran

1	1	1	1	1	1	1	1	1	1	1

Karena Kolom 2 semua bernilai 1 maka ketika dilakukan perputaran sebanyak 4 kali akan tetap seperti nilai semula

1	1	1	1	1	1	1	1	1	1	1

   c. Kolom 3 : di putar kearah bawah sebanyak 10 putaran

0	0	0	0	0	0	0	0	0	0	0

Karena Kolom 3 semua bernilai 0 maka ketika dilakukan perputaran sebanyak 2 kali akan tetap seperti nilai semula

0	0	0	0	0	0	0	0	0	0	0

   d. Kolom 4 : di putar kearah bawah sebanyak 5 putaran

0	0	1	1	0	0	0	1	0	0	0

Putaran 1 : Lakukan perpindahan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	1	1	0	0	0	1	0	0

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	0	1	1	0	0	0	1	0

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	0	0	1	1	0	0	0	1

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	0	0	0	0	1	1	0	0	0

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	0	0	0	1	1	0	0

   e. Kolom 5 : di putar kearah bawah sebanyak 2 putaran

1	0	0	0	1	1	0	0	1	1	0

Putaran 1 : Lakukan perpindahan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	0	1	1	0	0	1	1

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	0	0	1	1	0	0	1

Kolom 6 : di putar kearah bawah sebanyak 4 putaran

1	1	1	1	0	1	0	0	0	1	0

Putaran 1 : Lakukan perpindahan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	1	1	1	0	1	0	0	0	1

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	1	1	1	0	1	0	0	0

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	1	1	1	0	1	0	0

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	1	0	1	1	1	1	0	1	0

f. Kolom 7 : di putar kearah bawah sebanyak 5 putaran

1	0	0	0	0	0	0	1	0	1	0

Putaran 1 : Lakukan perpindahan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	0	0	0	0	1	0	1

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	0	0	0	0	0	1	0

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	0	0	0	0	0	1

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	0	0	0	0	0

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	1	0	0	0	0	0

g. Kolom 8 : di putar kearah bawah sebanyak 7 putaran

0	1	0	0	1	1	1	0	1	0	1

Putaran 1 : Lakukan perpindahan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	0	1	1	1	0	1	0

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	0	1	1	1	0	1

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	0	1	1	1	0

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	1	0	0	1	1	1

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	1	0	0	1	1

Putaran 6 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	1	0	1	0	1	0	1	0	0	1

Putaran 7 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 1 ke kolom 2, kolom 2 ke kolom 3, kolom 3 ke kolom 4 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	1	1	0	1	0	1	0	1	0	0

Dari putaran di atas yang telah dilakukan sehingga diperoleh hasil seperti tabel dibawah ini:

Tabel 3 Tahap setelah dilakukan Enkripsi

I	0	1	0	0	1	0	0	1
S	0	1	0	1	0	0	1	1
M	0	1	0	0	1	1	0	1
B	0	1	0	0	0	0	1	0
E	0	1	0	0	0	1	0	1
F	0	1	0	0	0	1	1	0
M	0	1	0	0	1	1	0	1
\	0	1	0	1	1	1	0	0
Q	0	1	0	1	0	0	0	1
D	0	1	0	0	0	1	0	0
H	0	1	0	0	1	0	0	0

I	0	1	0	0	1	0	0	1
S	0	1	0	1	0	0	1	1
M	0	1	0	0	1	1	0	1
B	0	1	0	0	0	0	1	0
E	0	1	0	0	0	1	0	1
F	0	1	0	0	0	1	1	0
M	0	1	0	0	1	1	0	1
****	0	1	0	1	1	1	0	0
Q	0	1	0	1	0	0	0	1
D	0	1	0	0	0	1	0	0
H	0	1	0	0	1	0	0	0

Maka Hasil Enkripsinya adalah : **ISMBEFM\QDH**

3.3. Proses 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.

Tabel 4 Hasil Enkripsi

I	0	1	0	0	1	0	0	1
S	0	1	0	1	0	0	1	1
M	0	1	0	0	1	1	0	1
B	0	1	0	0	0	0	1	0
E	0	1	0	0	0	1	0	1
F	0	1	0	0	0	1	1	0
M	0	1	0	0	1	1	0	1
\	0	1	0	1	1	1	0	0
Q	0	1	0	1	0	0	0	1
D	0	1	0	0	0	1	0	0
H	0	1	0	0	1	0	0	0
Key	11	3	10	5	2	4	5	7

Lakukan putaran pada setiap kolom dari bawah ke atas sebanyak kunci yang di berikan.

a. Kolom 1 : di putar kearah atas sebanyak 11 putaran

0	0	0	0	0	0	0	0	0	0	0

Karena Kolom 1 semua bernilai 0 maka ketika dilakukan perputaran sebanyak 11 kali akan tetap seperti nilai semula

0	0	0	0	0	0	0	0	0	0	0

b. Kolom 2 : di putar kearah atas sebanyak 3 putaran

1	1	1	1	1	1	1	1	1	1	1

Karena Kolom 2 semua bernilai 1 maka ketika dilakukan perputaran sebanyak 4 kali akan tetap seperti nilai semula

1	1	1	1	1	1	1	1	1	1	1

c. Kolom 3 : di putar kearah atas sebanyak 10 putaran

0	0	0	0	0	0	0	0	0	0	0

Karena Kolom 3 semua bernilai 0 maka ketika dilakukan perputaran sebanyak 2 kali akan tetap seperti nilai semula

0	0	0	0	0	0	0	0	0	0	0

d. Kolom 4 : di putar kearah atas sebanyak 5 putaran

0	1	0	0	0	0	0	1	1	0	0

Putaran 1 : Lakukan perpindahan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom yang terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	0	0	0	0	1	1	0	0	0

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	0	0	1	1	0	0	0	1

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	0	1	1	0	0	0	1	0

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	0	1	1	0	0	0	1	0	0

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	0	1	1	0	0	0	1	0	0	0

e. Kolom 5 : di putar kearah atas sebanyak 2 putaran

1	0	1	0	0	0	1	1	0	0	1

Putaran 1 : Lakukan perpindahan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir

pindahkan kolom 1 ke kolom yang terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	0	1	1	0	0	1	1

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	0	0	1	1	0	0	1	1	0

f. .Kolom 6 : di putar kearah atas sebanyak 4 putaran

0	0	1	0	1	1	1	1	0	1	0

Putaran 1 : Lakukan perpindahan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom yang terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	1	1	1	0	1	0	0

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	1	1	1	0	1	0	0	0

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	1	1	1	0	1	0	0	0	1

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	1	1	1	0	1	0	0	0	1	0

g. Kolom 7 : di putar kearah atas sebanyak 5 putaran

0	1	0	1	0	1	0	0	0	0	0

Putaran 1 : Lakukan perpindahan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom yang terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	0	0	0	0	0

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	0	0	0	0	0	1

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	0	0	0	0	0	1	0

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	0	0	0	0	1	0	1

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	0	0	0	0	0	1	0	1	0

h. Kolom 8 : di putar kearah atas sebanyak 7 putaran

1	1	1	0	1	0	1	0	1	0	0

Putaran 1 : Lakukan perpindahan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom yang terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	1	0	1	0	1	0	1	0	0	1

Putaran 2 : dari hasil yang sudah diperoleh pada putaran 1 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	1	0	0	1	1

Putaran 3 : dari hasil yang sudah diperoleh pada putaran 2 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	1	0	0	1	1	1

Putaran 4 : dari hasil yang sudah diperoleh pada putaran 3 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	1	0	0	1	1	1	0

Putaran 5 : dari hasil yang sudah diperoleh pada putaran 4 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	1	0	0	1	1	1	0	1

Putaran 6 : dari hasil yang sudah diperoleh pada putaran 5 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom 1 ke kolom terakhir, dan hasilnya akan terlihat seperti tabel dibawah ini :

1	0	1	0	0	1	1	1	0	1	0

Putaran 7 : dari hasil yang sudah diperoleh pada putaran 6 dilakukan lagi putaran dengan cara memindahkan bit dari kolom 11 ke kolom 10, kolom 10 ke kolom 9, kolom 9 ke kolom 8 dan seterusnya dan yang terakhir pindahkan kolom terakhir ke kolom 1, dan hasilnya akan terlihat seperti tabel dibawah ini :

0	1	0	0	1	1	1	0	1	0	1

Dari putaran di atas yang telah dilakukan sehingga diperoleh hasil seperti tabel di bawah ini :

Tabel 5 Hasil Dekripsi

N = 4E	0	1	0	0	1	1	1	0
E = 45	0	1	0	0	0	1	0	1
T = 54	0	1	0	1	0	1	0	0
T = 54	0	1	0	1	0	1	0	0
I = 49	0	1	0	0	1	0	0	1
M = 4D	0	1	0	0	1	1	0	1
A = 41	0	1	0	0	0	0	0	1
R = 52	0	1	0	1	0	0	1	0
I = 49	0	1	0	0	1	0	0	1
N = 4E	0	1	0	0	1	1	1	0
A = 41	0	1	0	0	0	0	0	1

Maka hasil dekripsinya adalah : NETTIMARINA

KESIMPULAN

Dengan adanya kesimpulan dan saran ini dapat diambil suatu perbandingan yang akhirnya dapat memberikan perbaikan-perbaikan pada masa yang akan datang. Adapun kesimpulan yang penulis peroleh adalah sebagai berikut:

1. Dalam proses pembuatan sistem aplikasi yang baru dapat diketahui bahwa untuk menyusun suatu program yang baik, tahap-tahap yang perlu dilakukan adalah dengan mempelajari sistem yang akan dirancang tersebut, kemudian mendesain suatu sistem yang dapat mengatasi masalah serta mengimplementasikan sistem yang didesain.
2. Sebuah sistem baru akan sangat berguna bila dipakai dalam sebuah *database* yang mempunyai data yang besar.
3. Dengan ditempatkannya kriptografi dalam sebuah *file* didalam *internet* akan semakin meningkatkan *file* tersebut dari orang yang tidak berkepentingan.
4. Dengan menggunakan sistem aplikasi ini, maka diharapkan *user* dapat dengan mudah melakukan enkripsi *file* dalam penyimpanan diinternet.

DAFTAR PUSTAKA

[1]. Hanson Prihantoro Putro, Teknik Kriptografi Block Cipher dengan VBR (Perputaran Bit Vertikal), STEI ITB, Bandung, 2007.
[2]. Avon Budiyono, Enkripsi Data Kunci Simetris dengan Algoritma Kriptografi LOKI97, Institut Teknologi Bandung, Bandung, 2004.
[3]. Irawan, Budhi, Jaringan Komputer, Graha Ilmu, Yogyakarta, 2005.
[4]. Maman Abdurohman, Analisis Performansi Algoritma Kriptografi RC6, Institut Teknologi Bandung, Bandung, 2002.
[5]. Rinaldi Munir, Kriptografi, Informatika, Bandung, 2006.
[6]. Nugroho, Bunafit , PHP dan MYSQL Dengan Editor DreamweaverMX, Andi, Yogyakarta, 2004.
[7]. Yusuf Kurniawan, Kriptografi: Keamanan Internet dan Jaringan Komunikasi, Informatika, Bandung, 2004.
[8]. Tonni Limbong, Parasian DP Silitonga, Testing the Classic Caesar Cipher Cryptography using of Matlab, International Journal Of Engineering Research & Technology, Vol 6, Issue 2, p 175-178, 2017.
[9]. http://www.sumut.com/download/algoritma_vbr.pdf tanggal akses 1 Mei 2011 jam 19.56 WIB