IMPLEMENTASI ALGORITMA VERTICAL BIT ROTATION (VBR) PADA FILE TEKS

Yeffriansjah Salim
STMIK Indonesia; Jl P.Hidayatullah, Telepon/WA 081348000591
Jurusan Sistem Informasi, Banjarmasin
e-mail: yeffri_salim@yahoo.com

Abstrak
Kriptografi adalah suatu ilmu untuk menyembunyikan suatu informasi. Apabila seseorang menerima atau mengirim pesan pada jaringan, ada empat hal persoalan yang penting, yaitu kerahasiaan, autentikasi, keutuhan dan non repudiation. Kerahasiaan adalah bahwa data kita tidak dapat dibaca oleh orang yang tidak berkepentingan. Autentikasi memberi garansi keaslian data serta dengan siapa kita berhubungan. Keutuhan memberi garansi bahwa data tidak mengalami perubahan sewaktu dalam perjalanan, dan non repudiation berarti si pengirim informasi tidak dapat menyangkal bahwa pesan yang dikirim bukan darinya. Salah satu dari bagian kriptografi adalah fungsi hash satu arah. Hash adalah suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang acak. Kegunaan hash satu arah untuk mempermudah proses enkripsi menjadi cipher text dengan meningkatkan kesulitan perubahan ke plaintext. Salah satu fungsi hash yang paling banyak digunakan adalah Vertical Bit Rotation (VBR). Penelitian ini membuat model implementasi algoritma vertical bit rotation (VBR) pada file teks, mulai dari membuat file teks (plaintext), proses enkripsi pada metode perputaran VBR ini mengubah posisi bit 11, 4, 2, 5, 10, 9, 5, dan 7 pada karakter yang telah diubah dalam bentuk nilai biner, selanjutnya akan disimpan ke dalam file teks, melakukan proses dekripsi file teks menggunakan algoritma VBR, dan membandingkan plaintext dengan isi file teks hasil dekripsi menggunakan algoritma VBR. Hasil dari penelitian dengan menggunakan 30 sampel plaintext yang dibuat secara acak (random) menghasilkan nilai accuracy 86,67%.sebanyak 4 sampel data mengalami kegagalan informasi dan tidak sesuai dengan plaintext disebabkan proses konversi dari bilangan biner ke ASCII menjadi karakter ciphertext terutama nilai ASCII.
Kata kunci Algoritma VBR, Enkripsi dan File Teks.

Abstract
Cryptography is a science to hide information. When someone receives or sends messages on the network, there are four important issues, namely confidentiality, authentication, integrity and non-repudiation. Confidentiality is that our data cannot be read by unauthorized persons. Authentication guarantees the authenticity of the data and with whom we are connected. Wholeness guarantees that the data does not change while in transit, and non-repudiation means the sender of the information cannot deny that the message sent is not from him. One part of cryptography is a one-way hash function. Hash is a code from encryption which generally consists of random letters or numbers. The use of one-way hashes to simplify the encryption process into cipher text by increasing the difficulty of changing to plaintext. One of the most widely used hash functions is Vertical Bit Rotation (VBR). This study makes an implementation model of the vertical bit rotation (VBR) algorithm on text files, starting from creating a text file (plaintext), the encryption process in the VBR rotation method changes the bit positions 11, 4, 2, 5, 10, 9, 5, and 7 characters that have been converted into binary values, will then be saved into a text file, decrypting the text file using the VBR algorithm, and comparing the plaintext with the contents of the decrypted text file using the VBR algorithm. The results of the study using 30 plaintext samples that were randomly generated resulted in an accuracy value of 86.67%. As many as 4 data samples experienced information failure and did not match the plaintext due to the conversion process from binary numbers to ASCII into ciphertext characters, especially the ASCII.
Keywords VBR Algorithm, Encryption and Text Files

1. PENDAHULUAN

Perkembangan teknologi informasi menjadikan pertukaran data menjadi suatu permasalahan yang serius, setiap hari pertukaran data terjadi, dan bervariasi besarnya maupun jenisnya. Adakalanya data tersebut bersifat rahasia seperti data pribadi, data organisasi, ataupun data negara. Kerahasiaan ini perlu dijaga agar tidak ada orang yang menyalahgunakan data-data tersebut. Atas dasar itulah sebabnya kriptografi dikembangkan. [1] Kriptografi adalah suatu ilmu menyembunyikan informasi, sampai saat ini,

berbagai macam algoritma kriptografi, namun secara keseluruhan algoritma kriptografi dibagi menjadi dua yaitu klasik dan modern.

Sewaktu seseorang menerima atau mengirim pesan pada jaringan, terdapat empat buah persoalan yang sangat penting, yaitu kerahasiaan, autentikasi, keutuhan dan *non repudiation*. [2] Kerahasian adalah bahwa data kita tidak dapat dibaca oleh orang yang tidak berkepentingan. Autentikasi memberi garansi tentang keaslian data serta dengan siapa kita berhubungan. Keutuhan memberi garansi bahwa data tidak mengalami perubahan sewaktu perjalanan, dengan kata lain data yang dikirim adalah data yang diterima. Dan *non repudiation* yang berarti si pengirim tidak dapat menyangkal bahwa pesan yang dikirim bukan darinya.Salah satu dari bagian kriptografi adalah fungsi hash satu arah. Hash adalah suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang acak.. Salah satu fungsi hash yang paling banyak digunakan adalah Vertical Bit Rotation (VBR).

Batasan masalah dalam penelitian ini adalah :

- File yang digunakan adalah bertipe teks (TXT)
- Menerapkan algoritma kriptografi Vertical Bit Rotation (VBR) dengan model data 1 Byte / 8 bit
- Melakukan pergeseran bit data dengan variabel sebanyak 8 bit dengan nilai tetap / konstan dengan urutan pergeseran bit ke-1=11, bit ke-2=4, bit ke-3=2, bit ke-4=5, bit ke-5=10, bit ke-6=9, bit ke-7=5, dan bit ke-8=7.

[3] Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia dengan menggunakan teknik-teknik metematika. Dalam menjaga kerahasiaan data dengan kriptografi, data sederhana yang dikirim (plaintext) diubah ke dalam bentuk data sandi (ciphertext), kemudian data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja. Tentunya hal ini menyebabkan pihak lain yang tidak memiliki kunci tersebut tidak akan dapat membaca data yang sebenarnya sehingga dengan kata lain data akan tetap terjaga.

[4]Algoritma kriptografi Vertical Bit Rotation (VBR), dibuat oleh Hanson Prihantoro Putro tahun 2007 dalam tulisannya berjudul Teknik Kriptografi Block Cipher dengan VBR (Perputaran Bit Vertikal). Beberapa penelitian yang berhubungan dengan Algoritma Vertical Bit Rotation (VBR) telah dipublikasikan antara lain penelitian [5] Roni Sapto Purwandoko tahun 2010 dengan judul Aplikasi Penyimpanan *File Online* Dengan Enkripsi Menggunakan Modifikasi Algoritma *Vertical Bit Rotation* (Vbr) 32 Bit, Penelitian [6] Rudi Hartono tahun 2015 dengan judul Aplikasi Penyimpanan File Online Menggunakan Algoritma Vertical Bit Rotation (VBR) 32 Bit, Penelitian [7] Yohana Romian Febrianti Tamba tahun 2016 dengan judul Implementasi Algoritma Vertical Bit Rotation Pada Keamanan Data Nasabah (Studi Kasus : PT. Asuransi Allianz Life Indonesia), Penelitian [8] Ebiet Nico Citra tahun 2018 dengan judul Penerapan Algoritma Vertical Bit Rotation (VBR) Dalam Penyimpanan File Online, sedangkan penelitian saat ini yang dilaksanakan penulis adalah melakukan proses enksripsi dan dekripsi menggunakan File Teks (TXT), metode yang digunakan penelitian ini yaitu metode Algoritma Vertical Bit Rotation (VBR) sebagai metode enkripsi dari plaintext dalam sistem kriptografi dan menguji accuracy dari metode Algoritma VBR tersebut dengan cara membandingkan antara hasil dekripsi dengan plaintext, sedangkan model inputan yang menjadi plaintext menggunakan sistem acak (random).

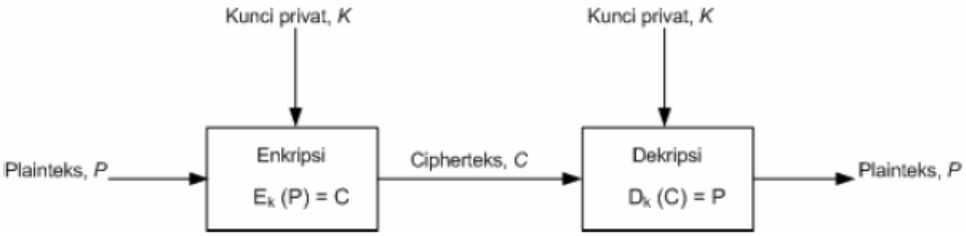
2. METODE PENELITIAN

Metodologi yang digunakan dalam melakukan penelitian ini menggunakan pengumpulan dokumen, studi pustaka dan eksperimen. Pengumpulan dokumen selayaknya guna mendapatkan dokumen input untuk diproses menghasilkan output serta dokumen untuk kelancaran penelitian. Dokumen yang digunakan pada penelitian ini seperti dokumen proses analisa sistem, desain proses, pembuatan kode program dan aplikasi sampai dengan pengujian aplikasi menggunakan Algoritma Vertical Bit Rotation (VBR). Studi pustaka bermanfaat mendapatkan referensi penelitian yang telah dilakukan sebelumnya yang berhubungan dengan penelitian saat ini dilaksanakan untuk diterapkan metode tersebut dalam penelitian. Eksperimen dilakukan dengan memasukan plaintext secara acak (random) dan disimpan ke dalam File Teks (TXT) untuk diproses dengan model Algoritma VBR baik saat enkripsi maupun dekripsi serta membandingkan hasil dekripsi dengan isi dokumen asal (plaintext).

2.1 Kriptografi Simetri (*Symetric Cryptography*)

[4] Pada sistem kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetri

adalah kriptografi kunci privat (*private key cryptography*) atau kriptografi konvensional (*conventional cryptography*).



Gambar 1 Kriptografi Simetri (*Symetric Cryptography*)

[9] Algoritma kriptografi simetri dikelompokkan menjadi dua kategori antara lain :

1. *Cipher* aliran (*stream cipher*)

Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit. Cipher aliran mengenkripsi satu bit setiap kali.

2. *Cipher* blok (*block cipher*)

Algoritma kriptografi beroperasi pada plaintext / ciphertext dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. *Cipher* blok mengenkripsi satu blok bit setiap kali.

2.2 Algoritma Kriptografi *Vertical Bit Rotation* (VBR)

[4]Algoritma kriptografi *Vertical Bit Rotation* (VBR) masuk dalam jenis kriptografi simetris dan masuk dalam kategori *cipher* blok. Pembuatan algoritma kriptografi ini lebih dilihat pada gambar 2.

Karakter Plainteks		Kode 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 2 Pembentukan blok penyandian pada algoritma kriptografi VBR

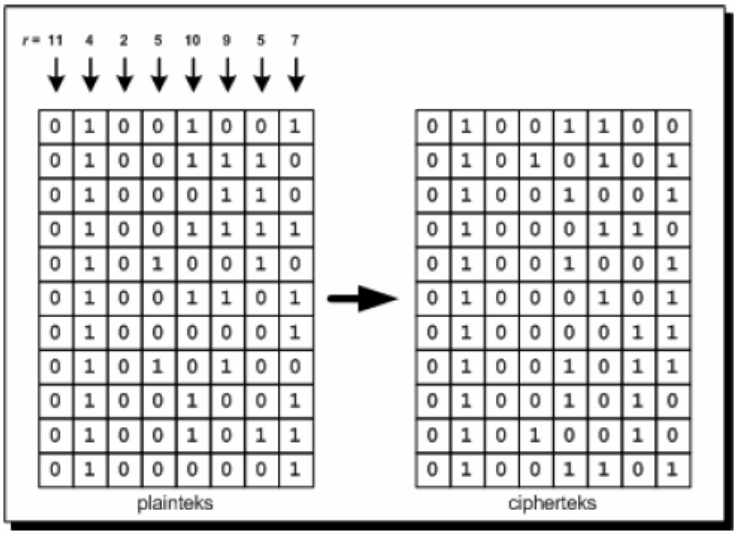
2.4 Proses Enkripsi

bertujuan pada membuat algoritma kriptografi modern namun memiliki kesederhanaan seperti algoritma kriptografi klasik.

2.3 Pembentukan Blok

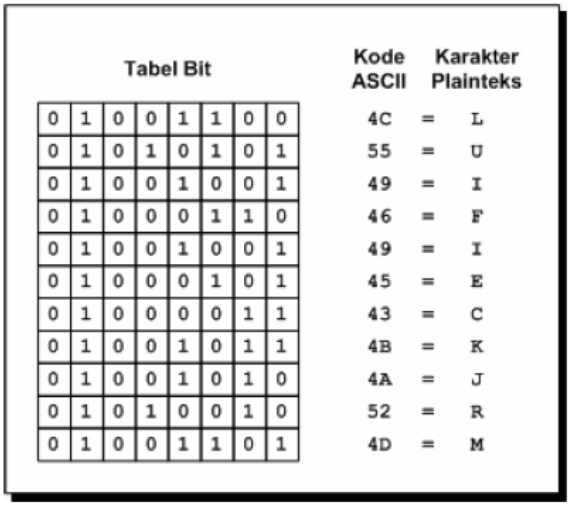
[10] Algoritma kriptografi VBR menggunakan blok dengan ukuran maksimal 256 byte. Namun untuk mendapatkan satu blok, tidak perlu dilakukan *padding* karena tanpa *padding* pun algoritma kriptografi ini masih dapat berjalan. Pertama-tama, sebuah arsip yang akan disandikan dibaca bit-bitnya, lalu dibagi sesuai dengan ukuran blok penyandian yaitu sebesar *N* byte. Dari satu blok, dipecah lagi per satu buah karakter, yaitu 8 bit, lalu pecahan-pecahan tersebut diurutkan secara vertikal. Sehingga didapatkan sebuah tabel bit yang terdiri dari 8 kolom dan *N* baris untuk *N* adalah jumlah (ukuran) blok penyandian. Apabila blok penyandian berukuran 256 byte, maka akan didapatkan tabel bit berukuran 8 kolom dan 256 baris. Sebagai contoh dapat

Proses enkripsi diterapkan bagi setiap blok penyandian, blok per blok dari bit data biner, sampai pada akhir blok, jika ukuran akhir blok lebih kecil dari blok penyandian yang ditentukan tidak akan diberikan padding. Enkripsi ini menggunakan pola menggeser dari atas ke bawah untuk setiap kolom-kolom pada tabel bit yang terbentuk saat membuat blok penyandian. Jumlah pergeseran atas ke bawah ditetapkan sebesar r bit pada setiap kolom yang sama, tetapi untuk masing kolom yang lainnya dapat dilakukan dengan besaran pergeseran yang berbeda-beda, pada tabel bit mestinya terdapat 8 kolom bit, 1 byte =1 karakter = 8 bit, sangat diperlukan 8 variabel nilai untuk menggeser bit-bit pada setiap kolom (*r*1, *r*2, *r*3, … *r*8). Contoh untuk enkripsi kata INFORMATIKA menggunakan nilai penggeser *r*1 hingga *r*8 ditetapkan sebesar 11, 4, 2, 5, 10, 9, 5, 7 hal ini dapat dilihat pada gambar 3.



Gambar 3 Proses enkripsi pada algoritma kriptografi VBR

Proses enkripsi ini akan menghasilkan ciphertext LUIFIECKJRM seperti dilihat pada gambar 4.

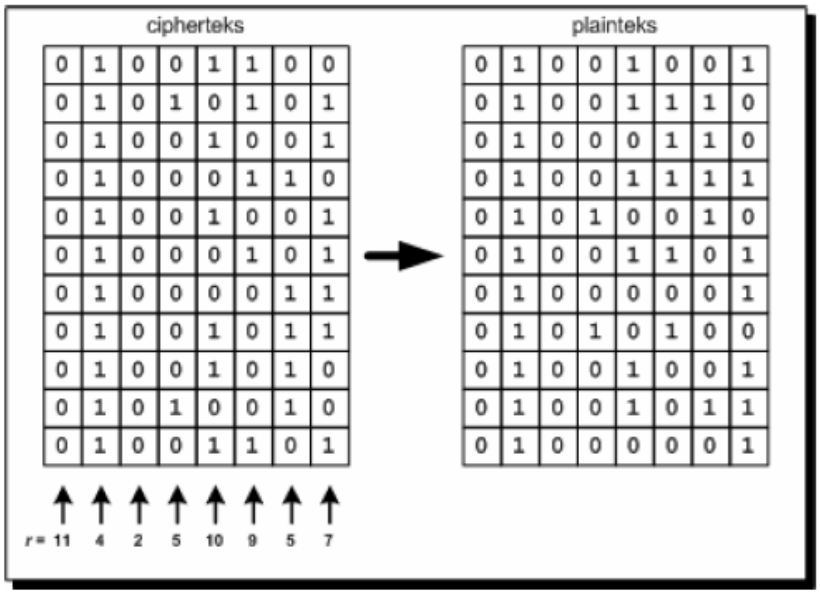


Gambar 4 Hasil enkripsi algoritma kriptografi VBR

Variabel rotasi perputaran 8 buah dapat diambil dari kunci yang terdiri dari 8 karakter (8 byte = 64 bit) yang diambil dari nilai ASCIInya.

2.5 Proses Dekripsi

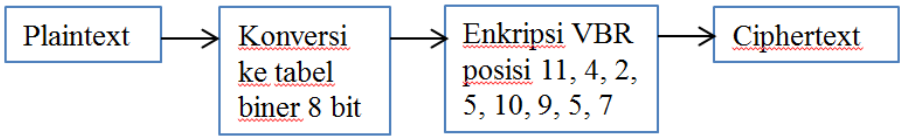
Sebagaimana halnya proses enkripsi yang telah dilakukan sebelumnya, proses dekripsi diterapkan pula pada setiap blok penyandian blok per blok, sampai dengan akhir blok, tidak ada padding pada akhir blok. Pergeseran tiap kolom pada tabel bit juga dilakukan hanya yang menjadi pembeda jika proses enkripsi pergeseran dari atas ke bawah, maka pada proses dekripsi dilakukan kebalikannya yaitu digeser dari bawah ke atas. Jumlah pergeseran kolom harus sama dengan saat melakukan proses enkripsi, jika tidak sama hasilnya akan tidak sempurna dan tidak akan didapatkan plaintext yang benar (hasil dekripsi berbeda dengan plaintext), hasil dari proses dekripsi dapat dilihat pada gambar 5.



Gambar 5. Proses dekripsi pada algoritma kriptografi VBR

Pada gambar 5. terlihat hasil dekripsi pada tabel bit dibandingkan dengan tabel bit plaintext memiliki kemiripan atau kesamaan sehingga informasi yang didapatkan sama.

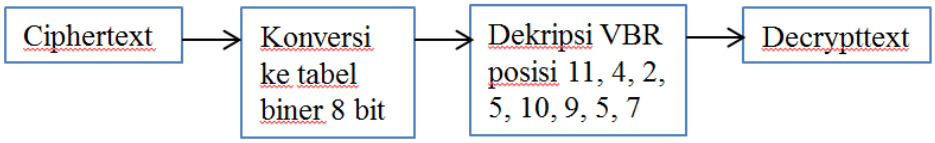
2.6 Tahapan Penelitian



Gambar 6. Proses Enkripsi

a. Proses Enkripsi :

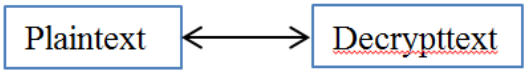
I. Menentukan Plaintext yang akan dijadikan bahan uji.
II. Setiap karakter dalam Plaintext akan diubah menjadi angka biner ke dalam tabel 8 bit.
III. Proses enkripsi perputaran bit posisi 11, 4, 2, 5, 10, 9, 5, 7 menggunakan metode VBR kemudian hasilnya dijadikan karakter, hasil enkripsi ini disimpan dalam bentuk file teks.



Gambar 7. Proses Dekripsi

b. Proses Dekripsi :

I. Menentukan Ciphertext yang akan dijadikan bahan uji.
II. Setiap karakter dalam Ciphertext akan diubah menjadi angka biner ke dalam tabel 8 bit.
III. Proses dekripsi perputaran bit posisi 11, 4, 2, 5, 10, 9, 5, 7 menggunakan metode VBR kemudian hasilnya dijadikan karakter, hasil dekripsi ini disimpan dalam bentuk file teks.

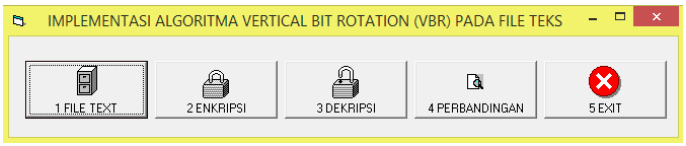


Gambar 8. Proses membandingkan

c. Proses membandingkan isi File Dekripsi dengan isi File Plaintext

3. HASIL DAN PEMBAHASAN

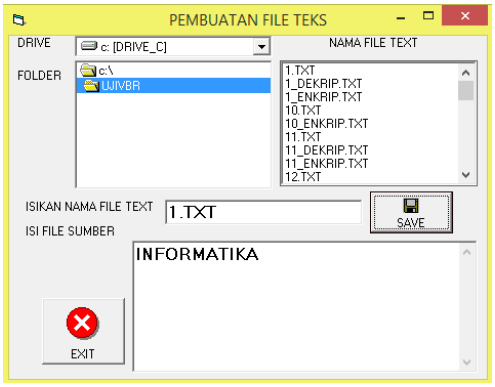
3.1 Menu Aplikasi



Gambar 9 Menu Aplikasi

Implementasi algoritma VBR pad file teks dimulai dari :

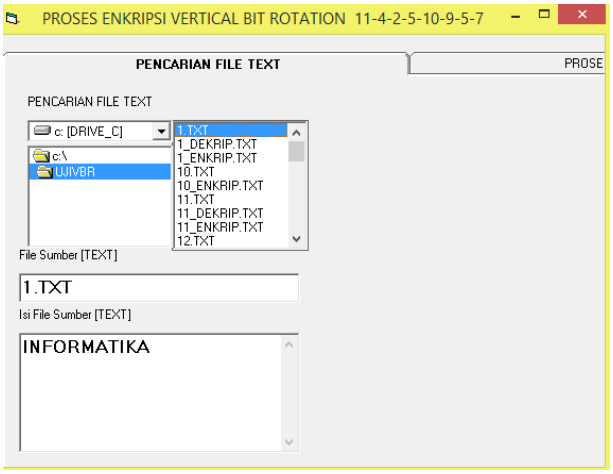
3.2 Membuat File Teks



Gambar 10 tampilan form membuat file teks

Pada menu ini dapat dilakukan memilih letak drive dan folder, dan dapat terlihat file teks pada folder tersebut, pada saat pertamakali yang perlu dilakukan adalah mengetikan nama file teks yang akan dijadikan file misalnya 1.TXT, setelah itu dapat diketikan isi file teks tersebut misalnya INFORMATIKA. Tombol SAVE digunakan untuk menyimpan file teks, sedangkan tombol EXIT digunakan untuk kembali ke menu sebelumnya.

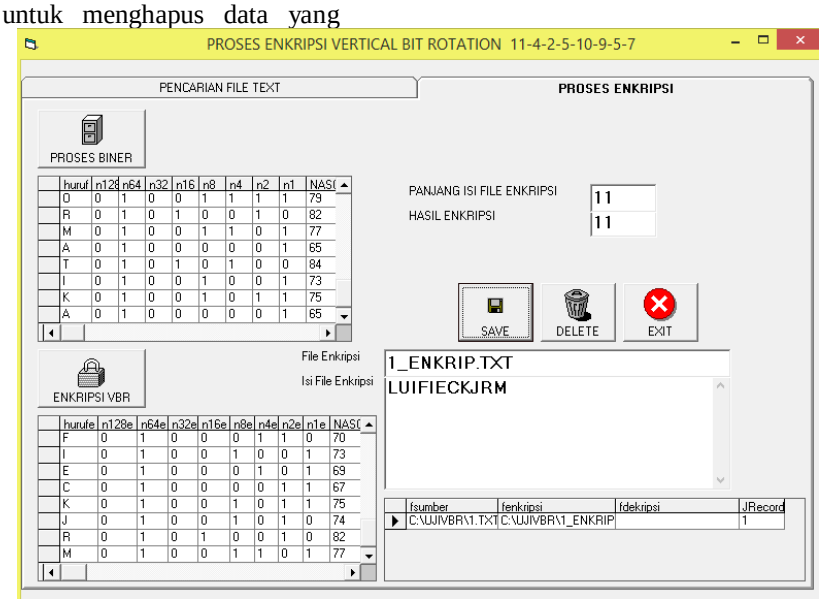
3.3 Proses Enkripsi



Gambar 11 pemilihan nama file teks yang akan dienkripsi

Pada menu ini dilakukan memilih file dengan mengklik salah satu dari nama file teks yang akan diproses untuk dienkripsi, secara otomatis akan ditampilkan isi file teks tersebut, selanjutnya dapat dilakukan dengan menekan tabulasi proses enkripsi seperti tampilan gambar 12, tombol PROSES BINER untuk mengkonversi setiap karakter ke bilangan biner 8 bit. Tombol ENKRIPSI VBR digunakan untuk mengkonversi bilangan biner ke bentuk perubahan pergeseran vertikal bit (atas ke bawah) dan secara otomatis untuk merubah nilai ascii bilangan tersebut menjadi karakter sebagi hasil enkripsi, hasil karakter yang telah terenkripsi ini

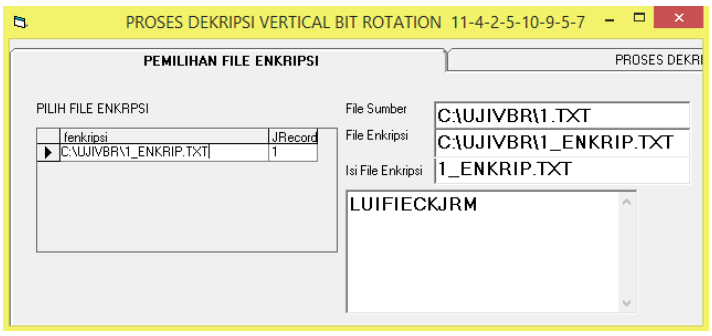
akan disimpan ke dalam bentuk file teks yang berbeda dengan nama file sumber ditambah dengan kata enkripsi misalnya nama file 1_ENKRIP.TXT, tombol SAVE untuk menyimpan hasil enkipsi, tombol DELETE untuk menghapus data yang tersimpan, sedangkan tombol EXIT digunakan kembali pada menu sebelumnya. Hasil enkripsi plaintext INFORMATIKA menjadi LUIFIECKJRM



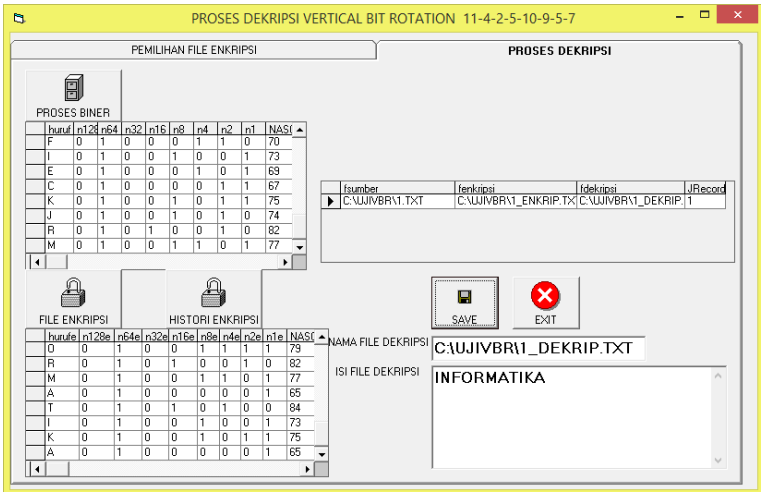
Gambar 12 proses enkripsi file teks (plaintext)

3.4 Proses Dekripsi

Pada menu ini dilakukan memilih file teks hasil enkripsi dengan mengklik salah satu dari nama file teks yang akan diproses untuk didekripsi, secara otomatis akan ditampilkan isi file teks tersebut, selanjutnya dapat dilakukan dengan menekan tabulasi proses dekripsi seperti tampilan gambar 14, tombol PROSES BINER untuk mengkonversi setiap karakter ciphertext ke bilangan biner 8 bit. Tombol FILE ENKRIPSI digunakan untuk mengkonversi jumlah karakter pada file ciphertext yang telah diubah menjadi bilangan biner ke bentuk perubahan pergeseran vertikal bit (bawah ke atas) dan secara otomatis untuk merubah nilai ascii bilangan tersebut menjadi karakter sebagai hasil dekripsi, sedangkan Tombol HISTORI ENKRIPSI digunakan untuk mengkonversi jumlah karakter pada file histori ciphertext yang telah diubah menjadi bilangan biner ke bentuk perubahan pergeseran vertikal bit (bawah ke atas) dan secara otomatis untuk merubah nilai ascii bilangan tersebut menjadi karakter sebagai hasil dekripsi. Hasil karakter yang telah terdekripsi ini akan disimpan ke dalam bentuk file teks yang berbeda dengan nama file sumber ditambah dengan kata dekripsi misalnya nama file 1_DEKRIP.TXT, tombol SAVE untuk menyimpan hasil dekripsi, sedangkan tombol EXIT digunakan kembali pada menu sebelumnya. Hasil dekripsi ciphertext LUIFIECKJRM didekripsi menjadi INFORMATIKA (plaintext).



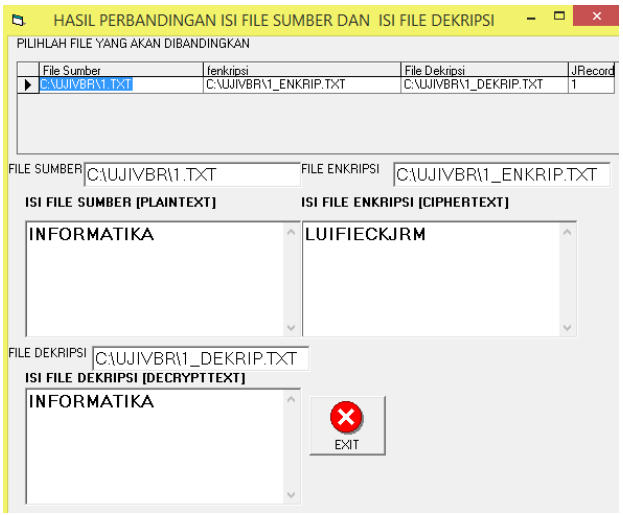
Gambar 13 pemilihan nama file teks enkripsi yang akan didekripsi



Gambar 14 proses dekripsi file teks (ciphertext)

3.5 Proses Perbandingan Plaintext dengan Hasil Dekripsi VBR

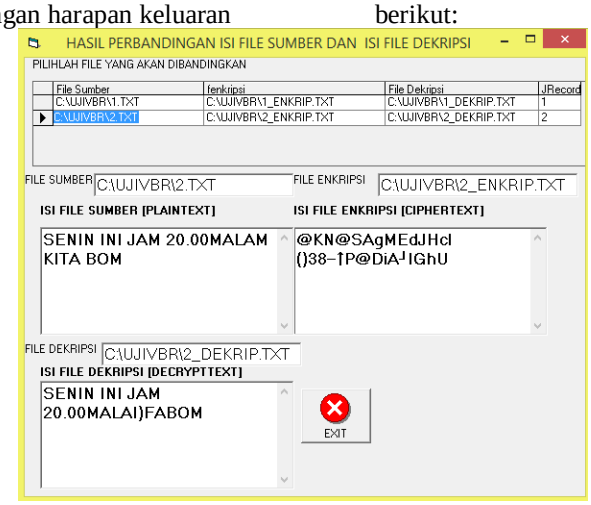
Perbandingan hasil dari proses dekripsi dan plaintext, sangat sederhana dengan mengklik satu kali pada data yang tersimpan pada tabel grid secara otomatis akan ditampilkan informasi nama dan isi file teks sumber (plaintext), nama dan isi file teks hasil enkripsi (ciphertext), nama dan isi file teks hasil dekripsi (decrypttext) seperti terlihat pada Gambar 15, sehingga terlihat jelas apakah proses tersebut memenuhi salah satu kaidah dari kriptografi tentang Integritas data (*data integrity*), yaitu memberikan jaminan bahwa untuk tiap bagian pesan tidak akan mengalami perubahan dari saat data dibuat/dikirim oleh pengirim sampai dengan saat data tersebut dibuka oleh penerima data.



Gambar 15 Proses Perbandingan Plaintext dengan Hasil Dekripsi VBR

3.6 Pengujian Sistem

Pengujian sistem yang telah dibuat mengenai accuracy menggunakan metoda blackbox. merencanakan isi dari plaintext, harapan keluaran dari proses dekripsi ciphertext, setelah itu akan dibandingkan antara isi plaintext dengan harapan keluaran dan hasil pengamatan. Pada kesempatan ini dilakukan pengujian dengan memasukan data secara acak (random) untuk isi file plaintext sebanyak 30 (tiga puluh) file dan didapat ketidaksesuaian sebanyak 4 (empat) data, lebih jelasnya dapat dilihat pada tabel berikut:

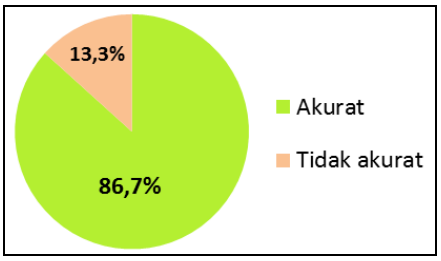


Gambar 16 hasil pengataman tidak akurat (plaintext < > decrypttext)

Tabel 1. Blackbox hasil pengamatan

Plaintext	Harapan Decrypttext	Hasil Pengamatan	Kesimpulan
SENIN INI JAM 20.00MALAM KITA BOM	SENIN INI JAM 20.00MALAM KITA BOM	SENIN INI JAM 20.00MALAI)FABOM	Tidak akurat
SENIN INI TEMPAT CAFE XYZ JAM21.00MALAM	SENIN INI TEMPAT CAFE XYZ JAM21.00MALAM	SENIN INI TEMPAT CAFE XYZ JAE2="0-ALAM	Tidak akurat
KITA BOM SENIN INI JAM 20.00MALAM	KITA BOM SENIN INI JAM 20.00MALAM	KITA BOM SENIN INI JAE >0"-aLAM	Tidak akurat
SENIN TGL 13/10/2020 KITA BOM JAM20.00MALAM	SENIN TGL 13/10/2020 KITA BOM JAM20.00MALAM	SENIN TGL 13/10/2020 KITA BOM BAM20-alAM	Tidak akurat

Sehingga pada eksprimen ini ada 4 data yang gagal memenuhi unsur kriptografi keutuhan / integritas data yaitu memberi garansi bahwa data tidak mengalami perubahan sewaktu perjalanan, dengan kata lain keseuaian data yang dikirim dengan data yang diterima, dapat dihitung accuracy hasil pengamatan ini sebesar 26/30=86,67% sedangkan tidak akurat sebesar 13,33%.



Gambar 17 Grafik accuracy pengujian sistem

4. KESIMPULAN

Implementasi Enkripsi File Teks Menggunakan Algoritma Kriptografi Vertical Bit Rotation (VBR) pada file teks ketika diaplikasikan dapat disimpulkan :

1. Hasil dari penelitian dengan menggunakan 30 sampel plaintext yang dibuat secara acak (random) menghasilkan nilai accuracy 86,67%.sebanyak 4 sampel data mengalami kegagalan informasi dan tidak sesuai dengan plaintext.
2. Metode Vertical Bit Rotation memiliki kekurangan antara lain jika nilai ASCII memiliki nilai yang tidak memiliki karakter yang khusus seperti nilai 00, 01, 09, 10, 13, 28, 29, 30, 31, dan 32. Karakter yang tidak teridentifikasi khusus ini menyebabkan informasi yang dienkripsi tidak dapat dikembalikan menjadi seperti semula (tidak sama dengan Plaintext).
3. Metode Vertical Bit Rotation akan berfungsi dengan baik apabila hasil enkripsi berupa nilai ASCII yang dapat direpresentasikan ke dalam karakter sehingga saat proses dekripsi dapat berjalan dengan sebagaimana mestinya.
4. Informasi yang dienkripsikan dapat menjamin kerahasiaan data yang disamarkan sehingga tidak akan dapat dibaca oleh orang yang tidak berhak membacanya sehingga aspek keamanan kriptografi seperti kerahasiaan, integritas data, otentifikasi, serta nirpenyangkalan terpenuhi.
5. Algoritma VBR diketahui suatu algoritma symmetric, yang menggunakan 64-bit kunci dan mempunyai 32 putaran untuk memproses setiap masing-masing *encrypt* atau *decrypt* operasi. Algoritmanya menggunakan 64 kunci bit Kriptografi VBR dapat dikatakan sangat dipercaya atau sangat menjamin keamanan data.
6. Proses enkripsi pada metode VBR ini mengubah posisi bit 11, 4, 2, 5, 10, 9, 5, dan 7 pada karakter yang telah diubah dalam karakter dari pembentukan nilai biner hasil perputaran bit, begitu pula dengan proses dekripsi dari konversi karakter ke nilai biner kemudian dilakukan perputaran bit kearah yang berlawanan saat proses enkripsi.

5. SARAN

Metode *Vertical Bit Rotation* memiliki kekurangan antara lain jika nilai ASCII memiliki nilai yang tidak memiliki karakter yang khusus seperti nilai 00, 01, 09, 10, 13, 28, 29, 30, 31, dan 32. Karakter yang tidak teridentifikasi khusus ini menyebabkan informasi yang dienkripsi tidak dapat dikembalikan menjadi seperti semula (tidak sama dengan Plaintext). Semoga tulisan penelitian ini dapat berkontribusi dalam penyempurnaan metode VBR untuk dapat mengatasi kelemahan ini di masa yang akan datang.

DAFTAR PUSTAKA

[1] Kurniawan, Yusuf .*Kriptografi: Keamanan Internet dan Jaringan Komunikasi*, Informatika, Bandung, 2004

[2] Munir, Rinaldi .Pengantar Kriptografi. Institut Teknologi Bandung, Bandung. 2004

[3] Munir, Rinaldi . *Kriptografi*. Informatika. Bandung. 2006.

[4] Prihantoro Putro, Hanson . *Teknik Kriptografi Block Cipher dengan VBR (Perputaran Bit Vertikal)*, STEI ITB, Bandung, 2007.

[5] Sapto Purwandoko, Roni .Aplikasi Penyimpanan *File Online*Dengan Enkripsi Menggunakan Modifikasi Algoritma *Vertical Bit Rotation* (Vbr) 32 Bit. Jurusan Teknik Informatika Fakultas Teknik Dan Ilmu Komputer Universitas Komputer Indonesia. 2010

[6] Rudi Hartono . Aplikasi Penyimpanan File Online Menggunakan Algoritma Vertical Bit Rotation (VBR) 32 Bit. Pelita Informatika Budi Darma, Volume : IX, Nomor: 1, Maret 2015

[7] Yohana Romian Febrianti Tamba . Implementasi Algoritma Vertical Bit Rotation Pada Keamanan Data Nasabah (Studi Kasus : PT. Asuransi Allianz Life Indonesia). Jurnal Ilmiah Infotek, Vol 1, No 1, Februari 2016.

[8] Ebiet Nico Citra . Penerapan Algoritma Vertical Bit Rotation (VBR) Dalam Penyimpanan File Online. MEANS (Media Informasi Analisa dan Sistem) Volume 3 No. 1, Juni 2018.

[9] Avon Budiyono, *Enkripsi Data Kunci Simetris dengan Algoritma Kriptografi LOKI97*, Institut Teknologi Bandung, Bandung, 2004.

[10] Kromodimoeljo, Sentot. Teori dan Aplikasi Kriptografi. SPK IT Consulting. 2010.