Pelita Informatika Budi Darma, Volume : VI, Nomor: 1, Maret 2014 ISSN : 2301-9425

PERANCANGAN PROGRAM KEAMANAN DATA FILE TEKS DENGAN MENGGUNAKAN ALGORITMA VERTICAL BIT ROTATION

Dhion Silalahi (1011476)

Mahasiswa Program Studi Teknik Informatika STMIK Budi Darma Medan
Jl. Sisingamangaraja No. 338 Sp. Limun Medan
www.stmik-budidarma.ac.id // Email : dhion.budidarma@gmail.com

ABSTRAK

Skripsi ini membahas tentang Implementasi Vertical BIT Rotation Untuk Aplikasi Enkripsi dan Dekripsi Data Pada File Text ataupun pengiriman data melalui jaringan. Vertical BIT Rotation merupakan cipher subtitusi ganda (multiple substitution cipher) yang melibatkan penggunaan kunci berbeda. Cipher alfabet majemuk dibuat dari sejumlah cipher alfabet tunggal, masing-masing dengan kunci yang berbeda.

Algoritma yang baik adalah algoritma yang tahan terhadap serangan. Kebaikan suatu algoritma dapat ditentukan dengan berapa banyak usaha yang dibutuhkan dalam memecahkan algoritma tersebut.

Kriteria aman itu persamaan matematisnya rumit sehingga sulit dipecahkan dengan metode analitik, biaya untuk memecahkannya tinggi melebihi nilai informasinya dan waktunya lama melebihi masa kadaluarsa informasi itu. Sehingga suatu algoritma dikatakan aman jika dapat memenuhi ketiga kriteria tersebut.

Keyword : Enkripsi, Dekripsi Transposisi, Bit Rotation

1. Pendahuluan

1.1. Latar Belakang Masalah

Enkripsi merupakan suatu proses pengubahan pesan asal menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang biasa digunakan seperti DES, Triple DES, Blowfish, IDEA dan sebagainya. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti dengan dalih 'faktor keamanan', katanya semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun bagi para pengguna mereka tidak memikirkan seberapa sulit algoritma dan aplikasinya, yang mereka inginkan adalah menjaga kerahasiaan data.

Ada 2 syarat untuk mengimplementasikan suatu system enkripsi yang aman. Pertama, true random bits (benar-benar hanya dihasilkan.sekali) dan kedua, key space yang besar untuk algoritma enkripsi tersebut. Jika kedua syarat dipenuhi, tidak masalah seberapa kompleks algoritma enkripsinya. Bahkan semakin sederhana semakin baik, karena semakin sederhana suatu algoritma, maka akan semakin sedikit proses komputasinya dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya. Kesederhanaan itulah yang ditawarkan oleh algoritma Vertical BIT Rotation Cipher, algoritma kriptografi yang secara teori dan praktek aman dari tangan-tangan penyadap, dan dikenal dengan sebutan 'unbreakable' algorithm.

1.2. Perumusan Masalah

Adapun rumusan masalah dalam penulisan skripsi ini adalah sebagai berikut :

1. Bagaimana menerapkan proses enkripsi dan dekripsi pada sebuah file teks?
2. Bagaimana menerapkan *Vertical BIT Rotation* yang diimplementasikan pada sebuah file teks?

1.3. Batasan Masalah

Adapun batasan masalah dalam pembuatan skripsi ini adalah sebagai berikut ini :

1. File yang bisa di Enkript adalah File yang bersifat plain text, yang berukuran max 1 MB
2. Algoritma yang digunakan adalah *Vertical BIT Rotation*
3. Jumlah putaran kriptografi tergantung dari kunci atau teks yang dimasukkan.
4. Bahasa Pemrograman Visual Basic 6.0

1.4. Tujuan dan Manfaat Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk menerapkan proses enkripsi dan dekripsi pada sebuah file teks Melakukan implementasi algoritma *Vertical BIT Rotation* pada sebuah file teks
2. Untuk menerapkan *Vertical BIT Rotation* diimplementasikan pada sebuah file teks
3. Untuk menerapkan pengamanan file teks pada sejumlah perangkat lunak.

Adapun manfaat dari penelitian ini adalah :

1. Untuk membuat sebuah program aplikasi keamanan data file teks pada algoritma *Vertical BIT Rotation*.
2. Untuk melakukan implementasi algoritma *Vertical BIT Rotation* pada sebuah file teks

3. Untuk mengamankan data teks pada sejumlah perangkat lunak.

2. Landasan Teori

2.1. Pengertian Data

Data berasal dari kata "datum" yang berarti fakta, yang mengandung arti dikembangkan dengan kenyataan yang dapat digambarkan dengan simbol, angka, huruf, dan sebagainya. (Aji Supriyanto *(PengantarTeknologiInformasi*,2005:6),

2.2. Algoritma Vertical BIT Rotation

Berikut akan dijelaskan secara singkat bagaimana teknik *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, dimana *Vertical BIT Rotation* akan lebih optimal jika pembagian dilakukan ke dalam 256 bytes. Kemudian bit-bit tersebut susun secara vertical berdasarkan karakter-karakter pembentuknya. Kini, telah mendapatkan sebuah 'tabel' bit yang terdiri dari 8 kolom dan 9 baris. Yang di proses dari sebuah kata "INFORMATIKA", adapun contoh enkripsi dapat dilihat pada gambar 1 berikut:

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

2.3. Sejarah Kriptografi

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa Mesir. **Mekanisme Kriptografi**

Suatu sistem kriptografi (kriptosistem) bekerja dengan cara menyandikan suatu pesan menjadi suatu kode rahasia yang dimengerti oleh pelaku sistem informasi saja. Pada dasarnya mekanisme kerja semacam ini telah dikenal sejak jaman dahulu. Bangsa Mesir kuno sekitar 4000 tahun yang lalu bahkan telah mempraktekkannya dengan cara yang sangat primitif.

Dalam era teknologi informasi sekarang ini, mekanisme yang sama masih digunakan tetapi tentunya implementasi sistemnya berbeda. Sebelum membahas lebih jauh mekanisme kriptografi modern, berikut ini diberikan beberapa istilah yang umum digunakan dalam pembahasan kriptografi.

1. *Plaintext*
   Plaintext (message) merupakan pesan asli yang ingin dikirimkan dan
   dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
2. *Chipertext*
   Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.
3. *Chiper*
   Chiper merupakan algoritma matematis yang digunakan untuk proses penyandian plaintext menjadi ciphertext.
4. *Enkripsi*
   Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan plaintext sehingga menjadi chipertext.
5. *Dekripsi*
   Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari chipertext.
6. *Kriptosistem*
   Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

Prosesnya pada dasarnya sangat sederhana. Sebuah plaintext (m) akan dilewatkan pada proses enkripsi (E) sehingga menghasilkan suatu ciphertext (c). Kemudian untuk memperoleh kembali plaintext, maka ciphertext (c) melalui proses dekripsi (D) yang akan menghasilkan kembali plaintext (m). Secara matematis proses ini dapat dinyatakan sebagai,

$$\mathbf{E(m) = c}$$
$$D(c) = m$$
$$D(E(m)) = m \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2,1)$$

Kriptografi sederhana seperti ini menggunakan algoritma penyandian yang disebut *cipher*. Keamanannya bergantung pada kerahasiaan algoritma penyandian tersebut, karena itu algoritmanya harus dirahasiakan. Pada kelompok dengan jumlah besar dan anggota yang senantiasa berubah, penggunaannya akan menimbulkan masalah. Setiap ada anggota yang meninggalkan kelompok, algoritma harus diganti karena anggota ini dapat saja membocorkan algoritma.

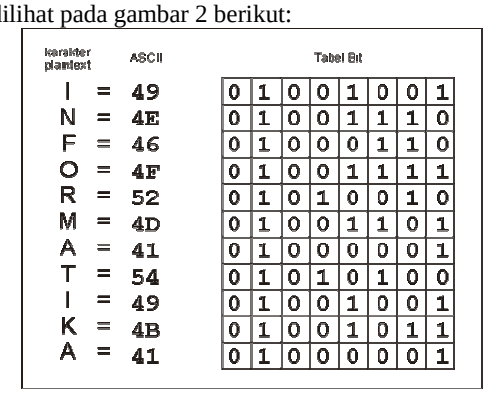
3. Analisa Pembahasan

Masalah keamanan merupakan salah satu aspek penting dari sebuah system informasi. Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data,

ataupun informasi adalah enkripsi. Di sini enkripsi dapat diartikan sebagai kode atau chiper . Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang dikirim. Sebuah chipper menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari suatu pesan asli (plaintext) menjadi *cryptogram* yang tidak di mengerti. Karena sistem chipper merupakan suatu sistem yang telah siap untuk diautomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

3.1. Analisa Vertical BIT Rotation

Berikut akan dijelaskan secara singkat bagaimana teknik *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, dimana *Vertical BIT Rotation* akan lebih optimal jika pembagian dilakukan ke dalam 256 bytes. Kemudian bit-bit tersebut susun secara vertical berdasarkan karakter-karakter pembentuknya. Kini, telah mendapatkan sebuah 'tabel' bit yang terdiri dari 8 kolom dan 9 baris. Yang di proses dari sebuah kata "INFORMATIKA", adapun contoh enkripsi dapat dilihat pada gambar 2 berikut:



Gambar 2. Tahap awal enkripsi/ dekripsi

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 di atas. Dan sebagai contoh diambil key berupa bilangan (11, 4, 2, 5, 10, 9, 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, seperti terlihat pada table 1 di bawah ini :

Table 1 : Tahap Awal Sebelum enkripsi/dekripsi

Key	11	4	2	5	10	9	5	7
I	0	1	0	0	1	0	0	1
N	0	1	0	0	1	1	1	0
F	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

Untuk Menjelaskan proses di atas dapat dilihat proses berikut ini :

1. Konversi Plainteks ke bentuk Binary
2. Set Binary menjadi 8 bit (8 Karakter)
3. Tempatkan Kunci ke setiap Bit Binary, sehingga dihasilkan informasi key dan binary seperti table 3.2 di bawah ini :

Table 2 : Tahap Enkripsi

Key	11	4	2	5	10	9	5	7
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

4. Lakukan putaran pada setiap kolom dari atas ke bawah sebanyak kunci yang diberikan

Tabel 3 : Tahap setelah dilakukan Tranparent (Enkripsi)

L	0	1	0	0	1	1	0	0
U	0	1	0	1	0	1	0	1
I	0	1	0	0	1	0	0	1
F	0	1	0	0	0	1	1	0
I	0	1	0	0	1	0	0	1
E	0	1	0	0	0	1	0	1
C	0	1	0	0	0	0	1	1
K	0	1	0	0	1	0	1	1
J	0	1	0	0	1	0	1	0
R	0	1	0	1	0	0	1	0
M	0	1	0	0	1	1	0	1

Maka Hasil Enkripsinya adalah : **LUIFIECKJRM**

3.3. Proses Dekripsi

Untuk proses dekripsinya, caranya tidak jauh berbeda. Jika pada proses enkripsi kita menggeser bit-bit ke bawah, untuk proses dekripsi, cukup menggeser bit-bit ciphertext ke atas sebanyak nilai-nilai key pada kolom yang bersesuaian, seperti terlihat pada table 4 di bawah ini :

Tabel 4 : Hasil Enkripsi

L	0	1	0	0	1	1	0	0
U	0	1	0	1	0	1	0	1
I	0	1	0	0	1	0	0	1
F	0	1	0	0	0	1	1	0
I	0	1	0	0	1	0	0	1
E	0	1	0	0	0	1	0	1
C	0	1	0	0	0	0	1	1
K	0	1	0	0	1	0	1	1
J	0	1	0	0	1	0	1	0
R	0	1	0	1	0	0	1	0
M	0	1	0	0	1	1	0	1
Key	**11**	**4**	**2**	**5**	**10**	**9**	**5**	**7**

4. Algoritma

A. Algoritma Enkripsi

Algoritma ini digunakan untuk melakukan enkripsi pada plain teks berdasarkan kunci yang dimasukkan

INPUT
- Nilai Kunci
- Karakter Plain Teks

OUTPUT
Hasil Enkripsi Plain Teks

PROSES

```
For i = 0 To sJum
   kar = sListAsal.List(i)
   sBinary = ""
   For j = 1 To Len(kar)
      sBinary = sBinary &
Mid(kar, j, 1)
   Next j
   sListTarget.AddItem
Chr(BinToDec(sBinary))
   sKata = sKata &
Chr(BinToDec(sBinary))
Next i
enc_ = sKata
For i = 1 To 8
   For j = 1 To jum
      sArrAsal(j) = sArr(j, i)
   Next j
   Putar_Atas sArrAsal, jum, i
   For j = 1 To jum
      sArr(j, i) = sArrAsal(j)
   Next j
Next i
For i = 1 To jum
   kata = ""
   For j = 1 To 8
      kata = kata & sArr(i, j)
   Next j
   List3.AddItem kata
Next i
```

B. Algoritma Dekripsi

Algoritma ini digunakan untuk melakukan enkripsi pada plain teks berdasarkan kunci yang dimasukkan

INPUT
- Nilai Kunci
- Karakter Chiper Teks

OUTPUT
Hasil Dekripsi plaint teks

PROSES

```
For i = 0 To sJum
   kar = sListAsal.List(i)
   sBinary = ""
   For j = 1 To Len(kar)
      sBinary = sBinary &
Mid(kar, j, 1)
   Next j
   sListTarget.AddItem
Chr(BinToDec(sBinary))
   sKata = sKata &
Chr(BinToDec(sBinary))
Next i
enc_ = sKata
For i = 1 To 8
   For j = 1 To jum
      sArrAsal(j) = sArr(j, i)
   Next j
   Putar_Atas sArrAsal, jum, i
   For j = 1 To jum
      sArr(j, i) = sArrAsal(j)
   Next j
Next i
For i = 1 To jum
   kata = ""
   For j = 1 To 8
      kata = kata & sArr(i, j)
   Next j
   List2.AddItem kata
Next i
```

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berdasarkan pembahasan yang dilakukan mengenai perangkat lunak pengolah gambar, maka penulis dapat mengambil beberapa kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk memproses setiap blok-blok bit tersebut agar tersusun secara vertikal berdasarkan karakter-karakter pembentuknya dengan menggunakan algoritma *Vertical BIT Rotation.*

2. Untuk proses Perangkat Lunak Enkripsinya berfungsi untuk menyembunyikan nilai-nilai bit dari karakter terkorespondasi, dan menggeser secara vertkal nilai-nilai bit yang sudah ada.
3. Untuk proses Perangkat Lunak Dekripsinya berfungsi untuk menggeser bit-bit chipertext ke atas sebanyak nilai-nilai key pada kolom yang bersesuaian.

5.2. Saran

Adapun saran yang dapat diberikan setelah melakukan pembahasan mengenai perangkat lunak proses pada enkripsi dan dekripsi ini adalah :

1. Melengkapi penerapan perangkat lunak dalam proses enkripsi dan dekripsi pada sebuah file teks.
2. Melengkapi penerapkan Algoritma *Vertical BIT Rotation* yang diimplementasikan pada sebuah file teks dan pada pengamanan file teks.
3. Perangkat Lunak ini masih belum sempurna, maka diharapkan pembaca dapat melalukan penambahan figure agar program ini agar menjadi lebih baik.

DAFTAR PUSTAKA

[1] Abdul Kadir, 2008 (***Pengenalan Sistem Informasi**,)"*

[2] Adi Kurniadi ***"Pemrograman Microsoft Visual Basic 6"***, Penerbit PT. Elex Media Komputindo Kelompok Gramedia, Jakarta.

[3] Aji Supriyanto, 2005 (***Pengantar Teknologi Informasi**,)*

[4] Al-Kindi 1987 (*"**A Manuscript on Deciphering Cryptographic Messages***")

[5] Gunawan Padia,, 2007 ("***Keamanan Data Dengan Kriptografi**)*

[5] Laudon, 2008 (***Sistem Informasi Manajemen: Mengelola Perusahaan Digital***)

[6] Munir, Rinaldi**,** 2005 ***("Diktat Kuliah IF5054 Kriptografi***", ITB, Bandung,)

[7] Munir, Rinaldi, 2006 (***" Kriptografi",*** Bandung, Penerbit Informatika)

[8] Tata Sutabri, 2005 (***Sistem Informasi Manajemen**,)*