IMPLEMENTASI VIGENERE CIPHER DENGAN RANDOM KEY METODE LFSR PADA TEKS

Masdiana Sagala[(1)] , Ayu Andira Sitorus[(2)]

[1] Teknik Informatika Unika Santo Thomas
Email : masdianasgl@gmail.com

[2] Teknik Informatika Unika Santo Thomas
Email : sitorusayu@gmail.com

Abstrak

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Perlindungan terhadap kerahasiaan data pun meningkat, salah satu caranya dengan penyandian data.

Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data dengan metode tertentu, dan pelakunya disebut cryptographer. Kriptografi disebut sebagai ilmu matematika karena didalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena dalam membuat suatu teknik kriptografi itu sendiri merupakan ciri tersendiri dari si pembuat dan memerlukan teknik khusus dalam mendisainnya. Sedangkan cryptanalysis adalah suatu ilmu dan seni memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya dan orang yang melakukannya disebut cryptanalyst.

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptoanalisis. Kriptoanalisis (cryptoanalysis), yaitu suatu ilmu dan seni yang dipelajari untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan atau aksi untuk memecahkan mekanisme kriptografi dengan cara mendapatkan plainteks atau kunci dari cipherteks yang digunakan untuk mendapatkan informasi berharga kemudian mengubah atau memalsukan pesan dengan tujuan untuk menipu penerima yang sesungguhnya memecahkan cipherteks.

Kata Kunci : Kriptografi, Vigenere Chiper, LFSR

1. Pendahuluan

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya dengan dengan penyandian data atau enkripsi.

Salah satu yang digunakan untuk mengamankan data adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah plaintext, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi ciphertext. Salah satunya algoritma yang dapat mengamankan data yang penulis bahas adalah Algoritma *Vigenere Chiper*.

Algoritma *Vigenere Cipher* merupakan salah satu dari algoritma kunci. Sampai saat ini, algoritma *Vigenere Cipher* masih dipercaya sebagai metode penyandian, kriptografi *Vigeere Cipher* menggunakan kunci yang sama untuk enkripsi dan dekripsi.

Linear Feedback Shift Register(LFSR) adalah shift register yang bit masukannya merupakan fungsi linear dari state sebelumnya. Satu-satunya fungsi linear pada bit satuan xor, oleh karena itu LFSR adalah shift register yang bit masukannya dibangkitkan oleh exclusive-or (XOR) dari bit dari keseluruhan nilai shift registrasi, LFSR ini digunakan untuk menciptakan sebuah kunci public secara otomotis, dan dengan adanya LFSR ini makan kunci yang digunakan pada *Vigenere Chiper* akan *digenerate* secara otomatis.

2. Sistem

Istilah sistem berasal dari bahasa Yunani yaitu *"Sistema"* yang artinya "Kesatuan". Sistem dapat terdiri dari beberapa sub sistem yang saling berhubungan untuk membentuk satu kesatuan hingga tujuan sasaran sistem dapat dicapai. Untuk mengetahui lebih dalam tentang sistem, berikut ini ada beberapa pengertian tentang sistem dari para ahli yaitu sebagai berikut :

Sistem adalah suatu kumpulan atau himpunan dari unsur, komponen atau variabel yang terorganisasi, saling tergantung satu sama lain dan terpadu (Tata Sutabri, 2005).

Sistem adalah suatu jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran tertentu (Rudy Adipranata, 2005).

Beberapa hal yang termasuk kedalam tahap perencanaan sistem diantaranya yang menyangkut kebutuhan-kebutuhan fisik yang digunakan untuk mendukung pengembangan sistem serta mendukung operasi setelah diterapkan.

3. Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata "kriptografi" dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti *secret* (rahasia) dan Graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain Kriptografi merupakan seni dan ilmu untuk menjaga keamanan data dengan metode tertentu, dan pelakunya disebut *cryptographer*. Kriptografi disebut sebagai ilmu karena di dalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena karena dalam membuat suatu teknik kriptografi itu sendiri merupakan ciri tersendiri dari si pembuat dan memerlukan teknik khusus dalam mendisainnya. Sedangkan *cryptanalysis* adalah suatu ilmu dan seni memecahkan ciphertext menjadi plaintext tanpa melalui cara yang seharusnya dan orang yang *melakukannya* disebut *cryptanalyst*.

Kriptografi juga dapat disebut dengan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Sebuah pesan rahasia harus terjaga keamanannya, salah satu cara dengan penyandian pesan yang bertujuan meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak ditujukan informasi tersebut kepadanya (Rinaldi Munir, 2004).

Menurut Kessler (2006), adapun tujuan sistem kriptografi adalah sebagai berikut :

a. Authentication
Proses menguji identitas seseorang.

b. Privacy/Confidentiality
Memastikan bahwa tidak ada yang dapat membaca pesan kecuali penerima yang dituju.

c. Integrity
Memastikan penerima yang menerima pesan tidak diubah dengan cara apapun.

d. Non-repudiation
Mekanisme yang membuktikan bahwa pengirim benar-benar mengirimkan pesan tersebut.

Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptoanalisis. Kriptoanalisis (*cryptoanalysis*), yaitu suatu ilmu dan seni yang dipelajari untuk memecahkan chiperteks menjadi plainteks tanpa mengetahui kunci yang digunakan atau aksi untuk memecahkan mekanisme kriptografi dengan cara mendapatkan plainteks atau kunci dari cipherteks yang digunakan untuk mendapatkan informasi berharga kemudian mengubah atau memalsukan pesan dengan tujuan untuk menipu penerima yang sesungguhnya, memecahkan cipherteks (Stephen Herlambang, 2011)

Secara sederhana adalah seseorang yang ingin menembus kerahasiaan dari sebuah kode dengan cara membangun algoritma baru yang bisa memecahkan algoritma yang sudah ada, pelakunya disebut kriptonalis. Munir (2004) mengatakan :"Jika seorang kriptografer mentransformasi plainteks dan chiperteks dengan suatu algoritma dan kunci maka sebaliknya seorang kriptonalis berusaha memecahkan chiperteks untuk menemukan plainteks atau kunci".

Setiap detiknya dalam dunia internet terjadi banyak sekali pertukaran informasi, Dan banyak pula pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Ada beberapa ancaman keamanan yang terjadi terhadap informasi di antaranya:

a. *Interuption*, adalah ancaman terhadap avaibability informasi, yaitu data yang ada dalam komputer dirusak atau dihapus sehingga saat informasi tersebut dibutuhkan tidak ada lagi.
b. *Interception*, adalah ancaman terhadap kerahasianan. Informasi yang ada disadap oleh orang yang tidak berhak mendapat akses ke komputer dimana informasi tersebut disimpan.

c. *Modification*, adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan dirubah sesuai keinginan orang tersebut.
d. *Fabrication*, adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menirukan atau memalsukan suatu informasi yang ada sehingga si penerima informasi mengira telah mendapatkan informasi dari pengirim yang sebenarnya.

Jadi, dari sini dapat di ketahui kriptografi diciptakan dengan tujuan, kerahasiaan, yaitu menjamin bahwa pesan dalam keadaan aman dari pihak yang tidak berhak, integritas data, yaitu menjamin bahwa pesan masih asli atau tidak dimanipulasi, autentikasi, yaitu megidentifikasi pesan dan pengirim pesan, dan non-repudiation, yaitu mencegah penyangkalan pihak yang berkomunikasi (menolak penyangkalan) (Ariyus, 2006).

4. *Linear Feedback Shift Register*

Menurut Stephen Herlambang (2011) menyatakan bahwa *Linear Feedback Shift Register(LFSR)* adalah shift register yang bit masukannya merupakan fungsi linear dari state sebelumnya. Satu-satunya fungsi linear pada bit satuan xor, oleh karena itu LFSR adalah shift register yang bit masukannya dibangkitkan oleh exclusive-or (XOR) dari bit dari keseluruhan nilai shift registrasi.

Inisial value dari LFSR dikenal dengan seed, dan karena operasi dari *register* bersifat deterministik, aliran nilai yang dihasilkan oleh *register* akan sepenuhnya ditentukan oleh state sekarang atau sebelumnya. Dengan begitu karena *register* memiliki jumlah state yang terbatas pasti akan terbentuk siklus yang berulang, akan tetapi LFSR yang memiliki fungsi umpan balik yang baik dapat memproduksi sekuens bit yang tampak acak dan memiliki siklus yang sangat penting

Konsep dasar dari LFSR yang artinya adalah "Register geser dengan umpan balik linier".Prosesnya adalah :

a. S1 sampai S4 diisi oleh bit-bit yang sudah ditentukan
b. Tahap pertama, S1 dan S4 akan di XOR-kan
c. S1-S4 digeser ke kanan sepanjang satu bit
d. Bit pertama akan dijadikan output
e. Bit hasil XOR antar S1 dan S4 (sebelum digeser) akan dimasukkan ke S4

5. Perancangan Sistem

5.1. Algoritma LFSR

Algoritma ini digunakan untuk memproses *Linear Feedback Shift Registers (LFSR)* yang akan digunakan sebagai kunci pada proses enkripsi

```
sJum = 8
For i = 1 To 8
   arTemporary(i) = arAsal(i)
Next i
For j = 1 To sKey
   sKet = ""
   For i = sJum To 1 Step -1
      If (i = sJum) Then
         arTemp(i) = arTemporary(1)
      Else
        arTemp(i) = arTemporary(i + 1)
      End If
   Next
   For i = 1 To 8
     sKet = sKet & arTemp(i)
   Next i
   For i = 1 To 8
      arTemporary(i) = arTemp(i)
   Next i
Next j
getLFSR = sKet
```

5.2. 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
```

5.3. Algoritma Dekripsi

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

INPUT

- Nilai Kunci
- Karakter Chiper Teks

OUTPUT

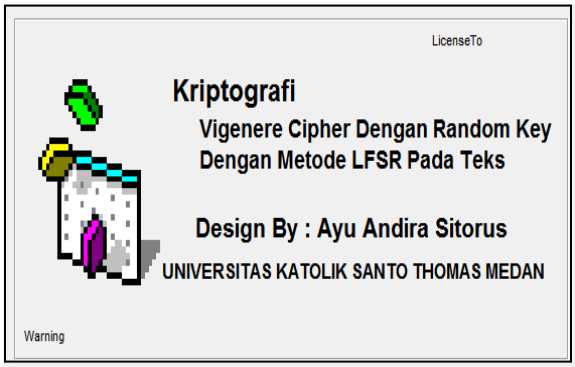
Hasil Dekripsi plaint teks

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
```

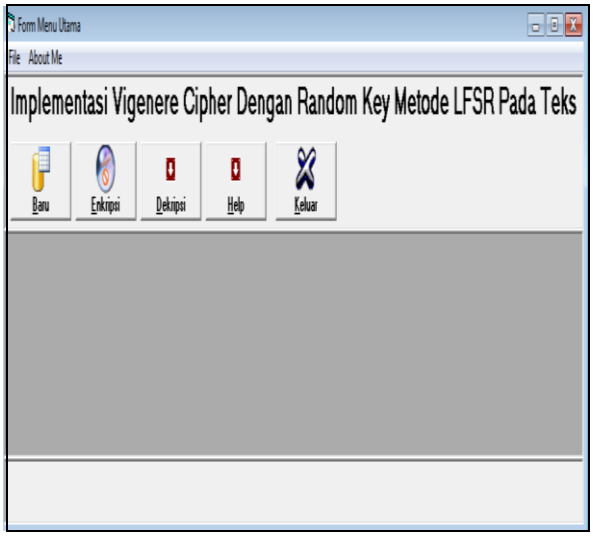
6. Implementasi

Form Aplikasi ini akan tampil pada saat Aplikasi pertama kali di jalankan. Untuk menjalankan perangkat lunak pengolahan gambar ini cukup dengan menjalankan file Kriptografi.exe, setelah dijalankan maka akan muncul tampilan flash. Implementasi nya dapat dilihat pada gambar 1.



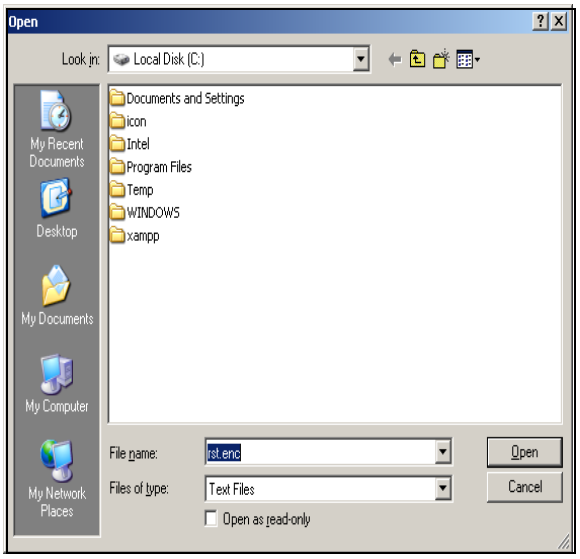
Gambar 1. Tampilan Flash

Form menu utama akan tampil setelah *user* menduobell klik pada From Aplikasi seperti pada gambar 1 digunakan untuk memilih Menu yang di inginkan oleh user. Implementasi nya dapat dilihat pada gambar 2.



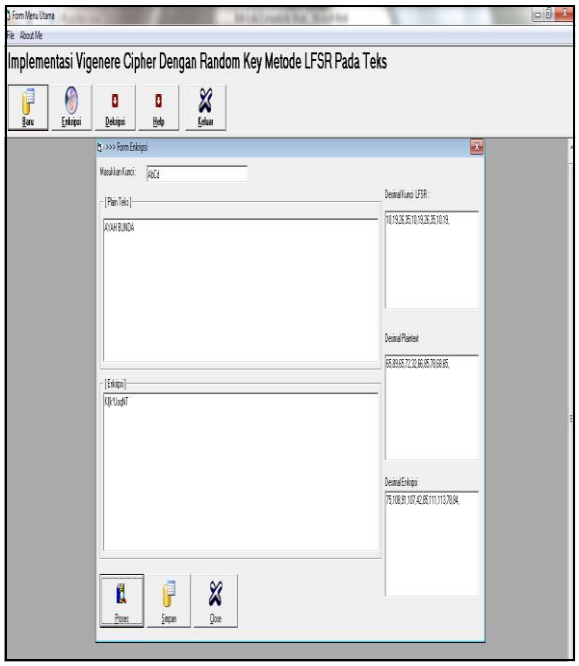
Gambar 2. Menu Utama

Form Enkripsi ini akan tampil setelah *user* menyimpan text yang akan digunakan untuk melakukan proses enkripsi pada informasi yang diambil dari sebuah file. Implementasi nya dapat dilihat pada gambar 3.



Gambar 3. Simpan File Enkripsi

Hasil proses enkripsi data dapat dilihat pada gambar 4.



Gambar 4. Form Hasil Enkripsi

7. Kesimpulan

Berdasarkan analisa dan perancangan yang dilakukan, maka dapat mengambil kesimpulan dari tugas akhir ini adalah sebagai berikut :

a. Vigenere Chiper akan lebih sulit di *crack* orang yang tidak berkepentingan karena kunci untuk enkripsi menggunakan teknik LFSR yang melakukan perputaran sebanyak 4 kali putaran
b. Aplikasi yang dirancang berfungsi untuk melakukan enkripsi dan dekripsi informasi dengan menggunakan algoritma *Vigenere Chiper dengan Metode Linear Feedback Shift Registers (LFSR)*

8. Saran

Adapun saran yang ingin di sampaikan penulis adalah sebagai berikut :

a. Penulis merasa bahwa Tugas Akhir ini belum sempurna, Implementasi vigenere chiper ini dapat di kembangkan lebih lanjut bukan hanya dengan file tapi harus bias juga dengan Microsoft Word dan excel .
b. Program ini dalam enkripsi dan dekripsi hanya melakukan batas local, dan diharapkan bias dikembangkan berbasis jaringan.

9. Daftar Pustaka

Tata Sutabri. 2005. *Sistem Informasi*. Andi Offset

Rudy Adipranata. 2005. *Perancangan Sistem Informasi*. Elex Media Komputindo.*http://repository.usu.ac.id/bitstream/123456789/20215/4/Chapter%20II*, Tanggal Akses 23-11-2012

http://id.wikipedia.org/wiki/Teks_biasa, Tanggal Akses 23-11-2012

Harrriansyah,2012,Pengertian Enkripsi dan Dekripsi (http://harriasnyah.blogspot.com/2012/04/pengertian-enkripsi-dan-dekripsi.html), tanggal akses : 09-12- 2012)

Ariyus, Pengantar Kriptografi, 2006 http://repository.usu.ac.id/bitstream/123456789/27198/4/Chapter%20II.pdf, Tanggal akses : 13-1-2013

Rinaldi Munir, 2004, Kriptografi, Bandung (http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Pengantar%20Kriptografi.pdf), tanggal akses : 13-1-2013

Stephen Herlambang, Makalah "Studi dan Analisis Grain Cipher", 2011(http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2009/2010/Makalah1/Makalah1_IF3058_2010_014.pdf), Tanggal akses : 23-3-1013

*Flourensia Sapty Rahayu, (*CRYPTOGRAPHY, Suplemen Bahan Ajar Mata Kuliah Proteksi dan Teknik Keamanan Sistem Informasi – IKI 83408T), Fakultas Ilmu Komputer Universitas Indonesia, 2005,

http://www.asciitable.com, Tanggal Akses 5-2-2013
http://www.Lookup Tables.com, Tanggal Akses 5-2-2013.