Perancangan Aplikasi Pengamanan File Dokumen Teks Dengan Menggunakan Algoritma Cipher Feedback

Muhammad Fauzi Dalimuthe
Teknik Informatika STMIK Budi Darma Medan Jl. Sisingamangaraja No. 338 - Medan
e-mail : mfd.dalimunthe@yahoo.com

Abstrak

Pada saat ini keamanan terhadap data yang tersimpan dalam komputer itu perlu salah satunya adalah pengamanan file dokumen tersebut dapat dilakukan adalah dengan kriptografi. Teknik Kriptografi dapat dimanfaatkan satu yang dapat dilakukan adalah dengan enkripsi yaitu proses penyandian sebelum file tersebut dikirim dan deskripsi yaitu proses penyandian sesdah file tersebut diterima, sehingga dengan proses tersebut file itu tetap dapat terjaga kerahasiaannya, dan hanya orang yang bersangkutan saja yang bisa mengetahuinya.

Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja dalam menjamin keamanan suatu informasi.

Kata Kunci *: Kriptografi, Algoritma Kriptografi, Cipher Feedback*

Abstract

At this time the security of the data stored on the computer is necessary, one of which is to secure the document file can be done is cryptography. Cryptography techniques can be used one that can be done is encryption, namely the encoding process before the file is sent and the description of the encryption process when the file is received, so that the file can still be kept confidential, and only the person concerned can know it.

Confidentiality is a service that is used to maintain information from any party that is not authorized to access it. Thus information will only be accessible to those entitled to guarantee the security of information.

Keywords ***:*** *Cryptography, Cryptographic Algorithms, Feedback Cipher*.

1. PENDAHULUAN

Keamanan suatu informasi pada jaman global ini makin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Salah satu aspek keamanan yang perlu dijamin adalah kerahasiaannya.Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.Teknik Kriptografi dapat dimanfaatkan dalam menjamin keamanan suatu informasi, salah satu yang dapat dilakukan adalah dengan enkripsi yaitu proses penyandian sebelum file tersebut dikirim dan deskripsi yaitu proses

penyandian sesdah file tersebut diterima, sehingga dengan proses tersebut file itu tetap dapat terjaga kerahasiaannya, dan hanya orang yang bersangkutan saja yang bisa mengetahuinya.

Metode *Cipher Feedback* adalah metode yang digunakan dalam sistem keamanan File Dokumen tersebut. Metode Cipher Feedback menggunakan sistem Shift Register, dimana yang diproses terlebih dahulu adalah Initialization Vector dalam algoritma Enkripsi dengan Kunci. Setelah diproses, bit yang dihasilkan akan melalui proses seleksi bit, biasanya bit – bit yang paling kiri, untuk selanjutnya dienkripsi dengan Plaintext untuk menghasilkan Ciphertext. Bit hasil seleksi yang digunakan tergantung besarnya bit blok plaintext yang diinput. Selanjutnya, setelah mendapatkan blok ciphertext, Enkripsikan antrian dengan kunci K. 8-bit paling kiri dari hasil enkripsi yang berlaku sebagai keysteam yang kemudian di XOR kan dengan karakter 8-bit dari plainteks menjadi karakter 8-bit pertama dari cipherteks.

2. METODOLOGI PENELITIAN

2.1. Kemanan File

Keamanan file dan informasi terdiri dari perlindungan terhadap aspek-aspek sebagai berikut :

a. Kerahasiaan adalah aspek yang menjamin kerahasiaan file atau informasi, memastikan bahwa file tersebut hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan file yang dikirim, diterima dan disimpan.
b. Integritas adalah aspek yang menjamin bahwa file tidak dapat diubah tanpa ada izin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini.

Ketersediaan adalah aspek yang menjamin bahwa file akan tersedia saat dibutuhkan, memastikan pengguna yang berhak dapat menggunakan informasi (asset yang berhubungan bila mana diperlukan [5].

2.2. Kriptografi

Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain.

Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasikan pengiriman pesan dan tangan digital dan keaslian pesan dengan siik jari digital [5]. Didalam kriptografi kita akan sering menemukan berbagai istilah atau terminology Algoritma yang artiya urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis.

Algoritma Kriptografi terdiri dari beberapa istilah yang harus diketahui yaitu :

a. Enkripsi : Enkripsi merupakan hal yang sangat penting dalam kriptografi yang merupakan pengamanan file dokumen yang dikirimkan terjaga kerahasiaannya. Nama lain untuk pesan adalah Plaintext yang dirubah menjadi kode-kode (cipher) yang tidak dapat dimengerti.
b. Deskripsi : Deskripsi merupakan kebalikan dari enkripsi, yaitu pesan yang telah dienkripsi dikembalikan kebentuk asalnya (Plaintext) disebut dengan deskripsi pesan.
c. Kunci : kunci yang dimaksud adalah kunci yang dipakai untuk melakukan enkripsi pada file dokumen indeks prestasi mahasiswa tersebut. Kunci tersebut terbagi atas dua jenis yaitu kunci pribadi (private key), dan kunci umum (publik key).

Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua himpunan yang berisi elemen-elemen plaintext dan himpunan yang berisi ciphertext. Enkripsi dan deskripsi merupakan fungsi yang memetakan elemen-elemen dua himpunan tersebut.(Munir, Rinaldi. 2006)

Misal :

P = Plaintext

C = Ciphertext maka,

Fungsi E memetakan P ke C

E (P) = C dan

Fungsi D memetakan C ke P

D (C) = P

Maka proses enkripsi kemudian deskripsi mengembalikan pesan ke pesan semula, dinyatakan dengan syarat yang harus dipenuhi dalam Kriptografi adalah : **D (E (P)) = P**

Kriptografi mengatasi masalah keamanan data file dokumen dengan menggunakan kunci yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi harus tetap terjaga kerahasiaannya. Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan K, maka fungsi enkripsi dan deskripsi dapat ditulis dengan :

Ek (P) = C dan Dk (C) = P

Dan kedua fungsi ini memenuhi

Dk (Ek (P)) = P

Keterangan :

P = Plaintext, C = Ciphertext, K = Kunci

Ek = Proses enkripsi menggunakan kunci K

Dk = Proses deskripsi menggunaka kunci K

2.3. Chiper Feedback

Metode Cipher Feedback adalah metode yang membutuhkan antrian yang sama dengan blok masukan. Membutuhkan antrian yang sama dengan blok masukan.

Metode Cipher Feedback ini mengenkripsikan data dengan cara :

a. Data dienkripsikan dalam unit yang lebih kecil dari pada ukuran blok.
b. Unit yang dienkripsikan dapat berupa bit per bit, bisa 2 bit, 3 bit dan seterusnya.
c. Bila unit yang dienkripsikan satu karakter setiap kalinya, maka mode CFBnya disebut CFB 8 bit.

Mode CFB 8-bit yang bekerja pada blok cipher berukuran 64-bit (setara dengan 8 byte). Algoritma enkripsi dengan mode CFB adalah sebagai berikut :

a. Antrian diisi dengan IV (initialiazation vector) seperti pada mode CBC.
b. Enkripsikan antrian dengan kunci K. 8-bit paling kiri dari hasil enkripsi. Berlaku sebagai keysteam yang kemudian di XOR kan dengan karakter 8-bit dari plainteks menjadi karakter 8-bit pertama dari cipherteks. Karakter cipherteks ini dikirim (pada aplikasi komunikasi data) atau disimpan (pada aplikasi penyimpanan data).

Salinan (copy) dari karakter cipherteks ini juga dimasukkan kedalam antrian (menempati 8 posisi bit yang paling kanan antrian), dan semua bit bit yang lainnya diantrian digeser kekiri menggantikan 8 bit pertama yang sudah digunakan.

a. Karakter plainteks berikutnya dienkripsikan dengan cara yang sama seperti pada langkah 2.
b. Deskripsi dilakukan sebagai kebalikan dari proses enkripsi.

Mode CBC memiliki kelemahan yaitu proses enkripsi hanya dapat dilakukan pada ukuran blok yang utuh sehingga mode CBC tidak efisien jika diterapkan pada aplikasi komunikasi data. Permasalahan ini dapat diatasi pada mode CFB. Mode CFB mengenkripsikan data dalam unit yang lebih kecil daripada ukuran blok. Proses enkripsi pada unit yang lebih kecil daripada ukuran blok ini membuat mode CFB berlaku seperti cipher aliran. (Schneier, Bruce. 2001).

Karena hal inilah, mode CFB dapat diterapkan pada aplikasi komunikasi data. Unit yang dienkripsi dapat berupa bit per bit. Bila unit yang dienkripsi berupa satu karakter setiap

kalinya, maka mode CFB ini disebut CFB 8-bit. Mode ini membutuhkan sebuah antrian yang berukuran sama dengan ukuran blok asukan. Secara formal, proses enkripsi mode CFB n-bit dapat dinyatakan sebagai berikut:

$$Ci = Pi \text{ Xor } MSBm(EK(Xi))$$
$$Xi+1 = LSBm\text{-}n(Xi) \,||\, Ci$$

sedangkan proses dekripsi dapat dinyatakan sebagai berikut:

$$Pi = Ci \text{ Xor } MSBm(DK(Xi))$$
$$Xi+1 = LSBm\text{-}n(Xi) \,||\, Ci$$

Keterangan:

Xi = isi antrian dengan X1 adalah IV
E = fungsi enkripsi
K = kunci
M = panjang blok enkripsi
N = panjang unit enkripsi
|| = operator penyambungan (*concatenation*)
MSB = Most Significant Byte
LSB = Least Significant Byte

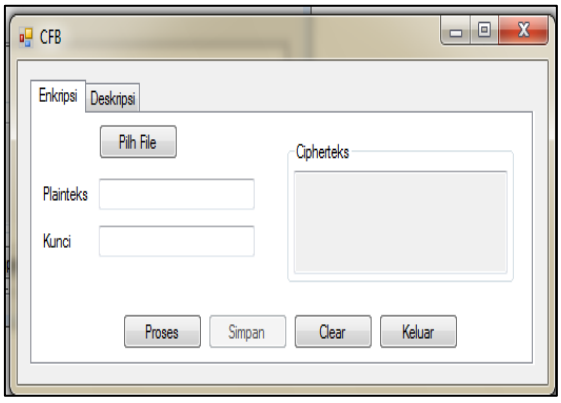
Mode CFB mempunyai keunikan tersendiri, yaitu untuk proses enkripsi dan dekripsi digunakan fungsi yang sama. Skema enkripsi dan dekripsi dengan mode CFB 8-bit.

3. HASIL DAN PEMBAHASAN

3.1. Hasil

Form Enkripsi berfungsi sebagai *form* awal yang digunakan untuk menyandikan pesan asli kedalam bentuk kode yang tidak bisa dibaca oleh pihak lain yaitu cipherteks.

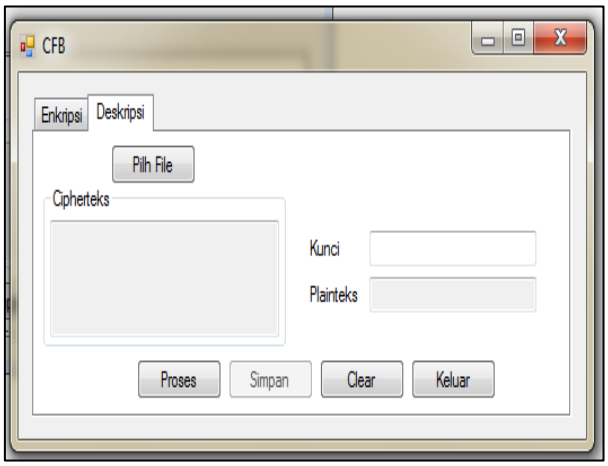
a. Pilih File
   Tombol Pilih File berfungsi untuk memilih file yang akan dienkripsi dan diproses.
b. Simpan
   Tombol Simpan berfungsi untuk menyimpan enkripsi yang telah diproses
c. Clear
   Tombol Clear berfungsi untuk membersihkan hasil proses enkripsi .
d. Keluar
   Tombol Keluar berfungsi untuk kembali ke menu design, dan keluar dari proses enkripsi.



Gambar 1. From Enkripsi

Form Deskripsi berfungsi sebagai *form* akhir yang digunakan untuk menyandikan pesan asli, yaitu kebalikan dari proses enkripsi dengan mengubah kode-kode yang tidak bisa dibaca kembali ke pesan asli.

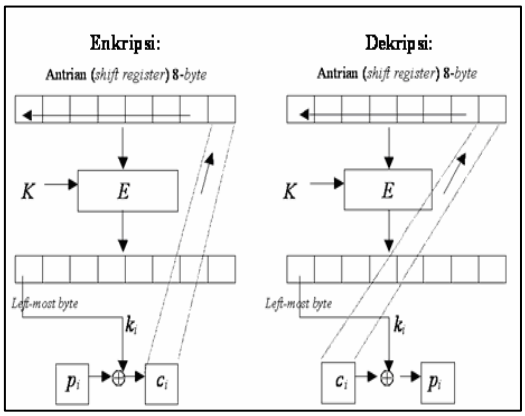
a. Pilih File
   Tombol Pilih File berfungsi untuk memilih file yang akan dideskripsi dan diproses.
b. Simpan
   Tombol Simpan berfungsi untuk menyimpan deskripsi yang telah diproses.
c. Clear
   Tombol Clear berfungsi untuk membersihkan hasil proses deskripsi.
d. Keluar
   Tombol Keluar berfungsi untuk kembali ke menu design, dan keluar dari proses deskripsi.



Gambar 2. From Dekripsi

3.2. Pembahasan

Dalam perancangan sistem dapat dinyatakan dalam proses penyandian dengan menggunakan proses enkripsi dan deskripsi dengan menggunakan Rumus sebagai berikut :



Gambar 3. Skema Enkripsi Dan Dekripsi

Pada saat File Dokumen tersebut akan dikrim kepada setiap pengguna, file tersebut di buat dalam bentuk protect, file yang telah diprotect akan dienkripsikan setelah itu hasilnya akan

dikirim pengguna. Setiap pengiriman file tersebut dan setiap pengguna akan memiliki password yang berbeda.

Nama	:Dedy Ardianto
Password	: IPMHS3,5
Kunci (K)	: I(01001001)
CFB	: 8 bit
Blok	: 64 bit
Plainteks (Pass)	: IPMHS3,5

Maka hasil yang diperoleh dari proses enkripsi adalah :

Plainteks : IPMHS3,5
01001001 01010000 01001101 01001000 01010011 00110011 00101100 00110101
Cipherteks : 01001111 01011100 01100111 00010100 11101001 01110010 01011010 00010011

Maka hasil deskripsi yang diperoleh adalah :

Cipherteks : 01001111 01011100 01100111 00010100 11101001 01110010 01011010 00010011
Plainteks : 01001001 01010000 01001101 01001000 01010011 00110011 00101100 00110101
IPMHS3,5

4. KESIMPULAN

Setelah penelitian dilakukan dan hasil pengujian diperoleh, maka penulis dapat menyimpulkan garis besar :

a. Aspek kerahasiaan pada Pengamanan File Dokumen yang menggunakan Metode Cipher Feedback terletak pada penyandian pesan yaitu “password”.
b. Aplikasi Pengamanan File Dokumen ini dapat melakukan enkripsi dan deskripsi password.
c. Metode Cipher Feedback pada Kriptografi Modern dapat diimplementasikan pada sebuah sistem informasi.

DAFTAR PUSTAKA

[1] Ariyus,Dony., 2005., Computer Security ., Andi Offset, Yogyakarta.
[2] Ariyus, Dony ., 2006., Kriptografi: Keamanan Data dan Komunikasi., Yogyakarta.
[3] Murni, Aniati, 1992., Pengantar Pengolahan Citra, Elexmedia Komputindo., Jakarta.
[4] Munir, Rinaldi., 2004., Buku Teks Ilmu Komputer Matematika Diskrit Edisi Ketiga, Informatika., Bandung.
[5] Munir, Rinaldi., 2006., Pengolahan Citra Digital dengan Pendekatan Algoritmik., Informatika. Bandung.
[6] Putra, Darma., 2009., Pengolahan Citra Digital ., Andi., Yogyakarta.
[7] Sutoyo. T., 2009., Teori Pengolahan Citra Digital., Andi., Yogyakarta.