ANALISA DAN PENERAPAN ALGORITMA DES UNTUK PENGAMANAN DATA GAMBAR DAN VIDEO

I Putu Herryawan
Program Studi Teknikinformatika,
Jurusan Ilmu Komputer,
Fakultas Matematika Danilmu Pengetahuan Alam,
Universitas Udayana
Email : putu.herry@cs.unud.ac.id

ABSTRAK

Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan kemajuan teknologi informasi namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia haruslah benar-benar diperhatikan.Untuk mengatasi masalah tersebut maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simteris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (*cipher*) yang digunakan adalah DES

Kata Kunci : *Kriptografi, Symmetric, and Cipher*

ABSTRACT

System security of data and data's secret represent one of important aspect in growth of information technology's progress but which enough regrettably is imbalance between every growth of a technology which is not accompanied with the growth of security's system. So that a lot of system which still be weak and have to be improved by security. Therefore data security which in character secret shall really paid to attention, to overcome the problem is hence needed an application of data security which can prevent and pacivy the data which we own from other people who have not business to acces it. One of them is method of algorithm of cryptography symmetric, because this algorithm use the same key at the conducting process of encryption and decryption, so that our data difficult to be understood and very quickly for the encryption data. Algorithm cryptography (cipher) used is DES

Keyword : *Cryptohraphy, Symmetric, and Cipher*

1. Pendahuluan

Pada dasarnya dalam membangun sebuah keamanan komputer diperlukan suatu sistem pengamanan data atau *file* yang kita miliki. Misalnya seseorang yang biasa menyimpan data-data penting ke dalam suatu *file* dengan karakter yang tidak terkode (*plaintext)*, sangatlah rawan apabila tidak berhati-hati. Apabila jika data tersebut di simpan dalam suatu komputer yang digunakan secara bebas, bagi siapa saja yang ingin menggunakannya karena seperti saat ini yang kita ketahui aktifitas pencurian data baik itu terhadap komputer yang terhubung pada suatu jaringan maupun tidak, sudah menjadi hal yang sering terdengar dan tidak asing lagi bagi kalangan intelektual khususnya dan masyarakat luas pada umumnya. Hal-hal yang berkaitan dengan pengamanan data-data penting tersebut haruslah benar-benar diperhatikan agar data yang akan disampaikan atau masih tersimpan dalam komputer kita tetap aman dari orang-orang yang tidak bertanggung jawab.

2. Metodelogi

Untuk dapat mengimplementasikan sistem diatas, maka secara garis besar di gunakan beberapa metode sebagai berikut :

1. Studi Literatur dan Teori Penunjang

Untuk memperoleh informasi dengan mempelajari buku-buku literatur atau karya lainnya yang membahas tentang kriptografi atau untuk menunjang pembuatan perangkat lunak yang berhubungan dengan materi penulisan skripsi.

2. Penerapan metode algoritma DES (*Data Encryption Standard),*dalam perancangan sistem.

3. Analisa permasalahan

Untuk mengetahui dan menentukan metode algoritma yang digunakan sehingga dapat menentukan cara yang paling efektif dalam penyelesaian suatu permasalahan dalam proses enkripsi maupun dekripsi.

4. Pembuatan aplikasi pengaman suatu file

Setelah menganalisa permasalahan, selanjutnya dilakukan perancangan atau pembuatan sistem dengan menggunakan model perancangan sistem yang telah diterapkan agar sistem hasilnya akan maksimal dan dapat digunakan oleh *user* dengan mudah.

5. Evaluasi program dengan melakukan pengujian dan pengoperasian sistem secara keseluruhan

Evaluasi program dan pengujian pada suatu sistem sangat diperlukan untuk mengetahui kestabilan sistem yang telah dibuat.

3. Pembahasan

Untuk mengatasi masalah keamanan dan kerahasiaan data dalam suatu komputer dapat dilakukan proses enkripsi dan dekripsi dengan menerapkan algoritma kriptografi. Dan hal tersebut dapat digunakan pada data-data atau *file-file* tertentu yang kita anggap penting. Sehingga dapat melindungi dan mengamankan data ataupun *file* yang kita miliki tersebut dari pemakai yang tidak berhak mengaksesnya. Pada pembuatan skripsi ini, penulis mengumpulkan data-data dari hasil pengamatan, konsultasi, dan studi literatur atas masalah-masalah yang terjadi.

3.1 Algoritma Kriftografi

Algoritma kriptografi disebut juga *cipher* yaitu fungsi matematika yang digunakan untuk melakukan enkripsi dan dekripsi suatu data atau pesan. Berdasarkan jenis kuncinya algoritma kriptografi dibagi menjadi dua bagian yaitu Algoritma kriptografi simetris (*Symmetric Cryptography Algorithm*) dan Algoritma kriptografi asimetris (*Asymmetric Cryptography Algorithm*)

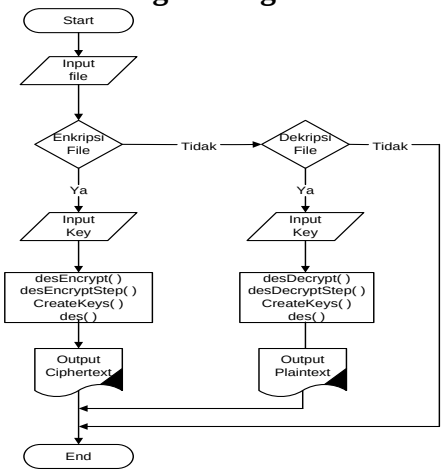
DES (*Data Encryption Standard)*

Algoritma enkripsi yang paling banyak digunakan didunia adalah DES *(Data Encryption Standard)* yang diadopsi oleh NIST (*National Institute of Standard and Technology)* sebagai standard pengolahan informasi Federal AS.

DES merupakan keamanan dasar yang dipublikasikan sejak 15 Januari 1977 dan sering digunakan dimana-mana, oleh karena itu ada kemungkinan DES akan tetap dilanjutkan penelitiannya sehingga menjadi suatu sistem enkripsi yang kuat dari segi keamanan data, sistem akses control dan *password*.

Gambar dibawah adalah gambar dari konsep dasar metode DES. Data dienkrip dalam blok-blok 64 bit menggunakan kunci 56 bit. DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi (biasa disebut dengan proses dekripsi).

3.2 Perancangan Program



Flowchart Proses Enkripsi dan Dekripsi Pada Metode DES

Illustrasi Metode DES

Misalkan suatu *plaintext* M = 0123456789ABCDEF, M dalam format heksadesimal (basis 16). Apabila ditulis dalam format biner M merupakan blok Dalam format biner pesan M dan kunci K dinyatakan sebagai berikut :

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100
1101 1110 1111

K = 0001 0011 0011 0100 0101 0111 0111 1001 1001 1011 1011 1100 1101
1111 1111 0001

Tahapan algoritma DES

Tahap 1 : Membuat 16 sub-kunci masing-masing panjangnya 48-bit

Kunci 64-bit dipermutasikan menurut Hasil permutasinya dapat dilihat sebagai berikut :

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111
11110001

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Selanjutnya hasil permutasi ini dipecah menjadi dua bagian, yakni bagian kiri C_0 dan bagian kanan D_0 yang masing-masing panjang 28 bit, yaitu :

C_0 = 1111000 0110011 0010101 0101111

D_0 = 0101010 1011001 1001111 0001111

Berdasarkan C_0 dan D_0 tersebut dibuat 16 blok C_n dan D_n, $1 \leq n \leq 16$. Setiap pasangan blok C_n dan D_n dibentuk dari pasangan blok sebelumnya C_{n-1} dan D_{n-1}, n = 1, 2, ..., 16, dengan menggunakan *schedule* "*left shift*" seperti pada tabel 2.3.

Sebagai contoh dari pasangan C_0 dan D_0 diperoleh :

C_0 = 1111000011001100101010101111

D_0 = 0101010101100110011110001111

C_1 = 1110000110011001010101011111

D_1 = 1010101011001100111100011110

.....

C_{16}= 1111000011001100101010101111

D_{16}= 0101010101100110011110001111

Untuk membentuk kunci K_n, $1 \leq n \leq 16$, dioperasikan tabel permutasi dari tiap pasangan C_nD_n. Setiap pasangan yang mempunyai 56 bit hanya dipilih 48 bit dengan tabel permutasi 2.4.

Contoh hasil permutasi untuk 16 kunci pertama tiap pasangan adalah sebagai berikut :

C_1D_1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

C_2D_2 = 1100001 1001100 1010101 0111111 0101010 1100110 0111100 0111101

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101

.....

.....

K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010

K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

Tahap 2 : Encode setiap 64-bit blok data

IP (*Initial Permutation*) dari 64 bit pesan M. Berdasarkan tabel 2.1 *Initial Permutation* susunan M menjadi sebagai berikut :

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100
1101 1110 1111

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111
0000 1010 1010

Hasil permutasi dibagi dua, yaitu bagian kiri L_0 32 bit, dan bagian kanan R_0 32 bit, yaitu :

L_0 = 1100 1100 0000 0000 1100 1100 1111 1111

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

Selanjutnya melalui proses iterasi 16 kali, untuk $1 \leq n \leq 16$, fungsi f yang mengoperasikan dua blok data 32 bit dan kunci K_n dari 48 bit untuk menghasilkan data blok 32 bit. Untuk n berjalan dari 1 sampai dengan 16 dihitung :

$L_n = R_{n-1}$

$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$

Hasil dari perhitungan ini adalah blok final untuk n = 16, yaitu $L_{16}R_{16}$. Sebagai contoh untuk n = 1, diperoleh :

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

$L_1 = R_0$ = 1111 0000 1010 1010 1111 0000 1010 1010

$R_1 = L_0 \oplus f(R_0, K_1)$

Untuk menghitung fungsi f, terlebih dahulu ekspansikan tiap blok R_{n-1} dari 32 bit menjadi 48 bit dengan tabel 2.5. Sebagai contoh hasil perhitungan $E(R_0)$ dari R_0 adalah sebagai berikut :

R_0 = 1111 0000 1010 1010 1111 0000 1010 1010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

Dan hasil dari perhitungan fungsi f adalah sebagai berikut :

K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 010101

$K_1 \oplus E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111

Hasil dari 48 bit atau 8 group dengan 6 bit per group disubtitusikan dengan S-Box (tabel 2.6). Misalkan hasil dari 48 bit ditulis dalam bentuk :

$K_n \oplus E(R_{n-1}) = B_1B_2B_3B_4B_5B_6B_7B_8$

dimana setiap B_i adalah group 6 bit.

Selanjutnya hitung :

$S_1(B_1)S_2(B_2)S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)S_8(B_8)$

dimana $S_i(B_i)$ adalah output dari S-Box ke –i.

Sebagai contoh untuk putaran pertama *output* S-Box diperoleh sebagai berikut

$K \oplus E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111

$S_1(B_1)S_2(B_2)S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)S_8(B_8)$ =

0101 1100 1000 0010 1011 0101 1001 0111

Langkah terakhir dari perhitungan fungsi f adalah permutasi P dari *output* S-Box untuk mendapatkan nilai akhir f :

$f = P(S_1(B_1)S_2(B_2)... S_8(B_8))$

Sebagai contoh hasil dari permutasi P dari tabel 2.7 didapat *output* 32 bit sebagai berikut :

$S_1(B_1)S_2(B_2)S_3(B_3)\ S_4(B_4)\ S_5(B_5)\ S_6(B_6)\ S_7(B_7)S_8(B_8)$ =

0101 1100 1000 0010 1011 0101 1001 0111

f = 0010 0011 0100 1010 1010 1001 1011 1011 $\rightarrow f(R_0, K_1)$

$R_1 = L_0 \oplus f(R_0, K_1)$ = 1100 1100 0000 0000 1100 1100 1111 1111 $\oplus$ 0010 0011 0100 1010 1010 1001 1011 1011 = 1110 1111 0100 1010 0110 0101 0100 0100

Untuk putaran berikutnya di dapat L2 = R1, dan harus dihitung R2 = L1 $\oplus$ f(R1,K2), diperoleh blok L_{16} dan R_{16} urutannya ditukar dan dipermutasikan dengan *final permutation* IP^{-1} (*inverse* dari IP*)*. Sebagai contoh misalkan pada putaran ke -16 diperoleh :

L_{16} = 0100 0011 0100 0010 0011 0010 0011 0100

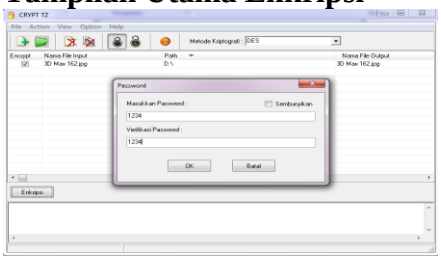
R_{16} = 00001010 0100 1100 1101 1001 1001 0101

Dibalik urutannya menjadi sebagai berikut :

$R_{16}L_{16}$ =00001010 01001100 11011001 10010101 01000011 01000010 00110010 00110100

Kemudian dipermutasikan dengan IP^{-1} diperoleh sebagai berikut : 85E813540F0AB405. Dengan demikian hasil enkripsi M = 0123456789ABCDEF adalah cipher teks C = 85E813540F0AB405. Proses dekripsi akan mengembalikan C = 85E813540F0AB405 menjadi M = 0123456789ABCDEF.

Tampilan Utama Enkripsi



Kesimpulan

Secara umum DES terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit yang mana satu kelompok saling berinteraksi satu dengan yang lainnya

Saran

Sistemkeamananmengalamiperkembangan yang sangatpesatdari system penyandiaan data ygmenggunakanenkripsi data 64 bit menjadi 128 bit, diharapkan biasdikembangkankearahenkripsi 128 bit.

Daftar Pustaka

Ariyus, Dony. (2006). ***Kriptografi Keamanan Data dan Komunikasi Edisi 1***.Yogyakarta: Penerbit Graha Ilmu.

Menezes, Alfred J, Paul C van Oorschot, Scott A, Vanstone. (1996). ***Handbook of Applied Cryptography***. CRC Press.

Munir, Rinaldi. (2006). ***Kriptografi***. Bandung: Penerbit Informatika Bandung.

Pranata, Antony. (2002). ***Pemrograman Borland Delphi 6 Edisi 4***. Yogyakarta: ANDI Yogyakarta.

Schneier, Bruce. (2006). ***Applied Cryptography 2nd***. John Wiley & Sons.

Shimizu, Akihiro, & Miyaguchi, Shoji. (1998). ***Fast Data Enchipherment Algorithm FEAL***. Trans. Of IECE of Japan.