ANALISA SISTEM KEAMANAN DATA MENGGUNAKAN METODE ENKRIPSI BLOWFISH DAN TRIPLE DES

Weldinar Sirait[1], R. Rumani[2], Tengku Ahmad Riza[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kriptografi merupakan suatu teknik penyandian data yang dapat digunakan untuk mengamankan data. Keamanan menjadi aspek yang utama dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi pihak tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Apalagi kalau data tersebut berada dalam suatu jaringan komputer yang terhubung dengan jaringan publik misalnya internet.

Untuk menjaga keamanan data satu caranya menggunakan metode kriptografi untuk mengenkripsi data tersebut. Pada tugas akhir ini digunakan algoritma Blowfish dan algoritma Triple DES. Kedua algoritma ini menggunakan kunci simetris dan berbentuk chiper blok. Sebagai user interface dibuat aplikasi dengan menggunakan Delphi. Aplikasi ini bisa mengenkripsi dan mendekripsi berbagai jenis file dan memproses perhitungan Avalanche Effect.

Nilai rata – rata Avalanche Effect dengan plaintext untuk Blowfish sebesar 43.638 %, 51.655%, 50.738% dan TripleDES 50,887%, 49.304%, 49.361% sedangkan Avalanche Effect dengan kunci untuk Blowfish sebesar 49.49%, 49.396%, 50.276% dan TripleDES 47.91%, 49.813%, 48.104% sehingga kedua algoritma kriptografi tersebut tergolong baik dalam menyandikan data. Dari data yang diambil lama waktu yang dibutuhkan untuk enkripsi dan dekripsi dengan metode Blowfish lebih cepat dibandingkan dengan metode TripleDES. Perbedaaan besarnya ukuran file berpengaruh pada waktu enkripsi maupun dekripsi dimana ukuran file berbanding lurus dengan lama proses enkripsi dan dekripsi artinya semakin besar ukuran filenya maka semakin lama pula waktu prosesnya. Faktor – faktor yang berpengaruh terhadap hasil chipertext setelah dilakukan proses enkripsi dengan menggunakan Algoritma Blowfish dan TripleDES antara lain plaintext dan kunci.

Kata Kunci : Kriptografi, Enkripsi, Dekripsi, Blowfish, Triple Des, Avalanche Effect

Abstract
Cryptography is a technique that can be used for data encryption to secure the data. Security has become a major aspect of an information system. A general information only for a particular party. Therefore it is very important to prevent it from falling to the other parties who are not interested. Moreover, if the data is in a network of computers connected to the public network such as the Internet.

To maintain the security of the data we can use cryptographic method to encrypt the data. In this final project used Blowfish algorithm and Triple DES algorithm. Both of these algorithms use a symmetric key and block cipher. As the user interface with the application created using Delphi. This application can encrypt and decrypt files and process various types of calculations Avalanche Effect.

Average plaintext for Avalanche Effect with Blowfish at 43,638%, 51,655%, 50,738% and TripleDES 50.88%, 49,30%, 49,36% while the Avalanche Effect with keys for Blowfish at 49.49%, 49,39%, 50,27% and TripleDES 47,91%, 49,81%, 48,10%. Both of the cryptographic algorithm can encrypt the data quite well. From data taken, time required for encryption and decryption with Blowfish method faster than TripleDES method. Differences affect the size of the file at the time of encryption and decryption where file size is proportional to the long process of encryption and decryption, means the larger the file size the longer the time process. Factors that affect the results of the ciphertext after encryption using the Blowfish algorithm and TripleDES include plaintext and key.

Keywords : Cryptography, Encrypt, Decrypt, Blowfish, Triple Des, Avalanche Effect

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data, bertujuan untuk menjaga kerahasiaan suatu pesan. Informasi yang dikirimkan harus terjaga kerahasiannya dan tetap asli tanpa dimodifikasi pada saat sampai di tujuan. Dalam metode kriptografi terdapat dua proses yaitu proses enkripsi dan dekripsi. Metode algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris dengan menggunakan *chiper blok.*

Pada penelitian sebelumnya dilakukan perbandingan dengan menggunakan algoritma *Rijndael* dan *Triple DES* (Muh Rizal, 2012). Kedua algoritma itu memiliki perbedaan dimana *Triple DES* menggunakan *cipher blok* sedangkan *rijndael* menggunakan *add round key*. Selain itu *Triple DES* menggunakan jaringan *Feistel* dan berorientasi bit sedangkan *Rijndael* tidak menggunakan *Feistel* dan beroperasi dalam *byte*.

Pada penelitian ini menggunakan algoritma *Blowfish* dan *Triple DES*. Kedua algoritma ini menggunakan kunci simetris, *blok cipher* dan jaringan *feistel*. Salah satu cara untuk mengetahui tingkat keamanan suatu algoritma kriptografi dapat dilakukan dengan cara menghitung nilai *Avalanche Effect* dari file yang telah terenkripsi. *Avalanche Effect* adalah menghitung perbedaan bit pada dua *chipertext* yang merupakan output dari hasil enkripsi dengan menggunakan algoritma kriptografi. Selain itu pengujian juga akan dilakukan dengan mengukur kinerja *Blowfish* dan *Triple DES* dari segi waktu enkripsi dan dekripsi.

1.2. TUJUAN

Tujuan pada penelitian tugas akhir ini adalah sebagai berikut :

1. Mengenkripsi berbagai jenis macam data .
2. Menganalisis tingkat keamanan dari algoritma kriptografi *Blowfish* dan *Triple DES* dengan menghitung nilai *Avalanche Effect*.
3. Menganalisis lama waktu proses enkripsi menggunakan algoritma *Blowfish* dan *Triple DES*.

1.3. RUMUSAN MASALAH

Berdasarkan latar belakang masalah diatas, identifikasi masalahnya adalah:

1. Bagaimana membangun aplikasi untuk menjalankan proses enkripsi dan dekripsi.
2. Bagaimana proses algoritma *Triple DES* dan *Blowfish*.
3. Mengukur performansi berdasarkan lama waktu enkripsi dan *avalanche effect*.

1.4. BATASAN MASALAH

Batasan masalah dalam penelitian dan pengembangan tugas akhir ini adalah:

1. Algoritma yang digunakan adalah *Blowfish* dan *Triple DES*.
2. Tidak membahas masalah jaringan dan trafiknya.
3. Aplikasi menggunakan bahasa pemrograman *Delphi*

1.5. METODE PENELITIAN

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

a. Studi literatur

b. Perancangan dan realisasi

c. Pengujian dan analisis implementasi

- Membuat aplikasi program yang dapat melakukan proses enkripsi dan dekripsi.
- Melakukan analisis cara kerja dalam proses pengenkripsian data dari kedua metode tersebut.
- Melakukan analisis kelebihan dan kekurangan dari kedua metode tersebut dalam proses pengenkripsian data

1.6. SISTEMATIKA PENELITIAN

Penulisan tugas akhir ini akan dibagi dalam beberapa bagian sebagai berikut:

1. **Bab I Pendahuluan**

   Berisi tentang latar belakang pembuatan ugas akhir, maksud dan tujuan pembuatan tugas akhir, pembatasan masalah, metodologi penulisan, serta sistematika yang digunakan dalam penulisan laporan tugas akhir.

2. **Bab II Dasar Teori**

   Berisi tentang penjelasan teoritis dalam berbagai aspek yang akan mendukung kearah analisis tugas akhir yang dibuat.

3. **Bab III Perancangan Sistem**

   Berisi penjelasan mulai dari proses desain hingga konfigurasi untuk implementasi sistem, serta skenario yang digunakan untuk melakukan pengujian.

4. **Bab IV Pengujian dan Analisis**

   Berisi analisis dari implementasi sistem sesuai skenario yang telah ditetapkan.

5. **Bab V Kesimpulan dan Saran**

   Berisi kesimpulan yang diperoleh dari serangkaian kegiatan terutama pada bagian pengujian dan analisis. Selain itu juga memuat saran-saran pengembangan lebih lanjut yang mungkin dilakukan.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

1. Dari data yang diambil lama waktu yang dibutuhkan untuk enkripsi dan dekripsi dengan metode *Blowfish* lebih cepat dibandingkan dengan metode *TripleDES*. Untuk *blowfish* enkripsi rata-rata 6157,504 ms sedangkan *triple des* rata-ratanya 17774,527 ms. Sedangkan untuk dekripsi, rata-rata *blowfish* 6393,478 ms dan dekripsi rata-rata *triple des* 17979,97 ms Perbedaaan besarnya ukuran file berpengaruh pada waktu enkripsi maupun dekripsi dimana ukuran file berbanding lurus dengan lama proses enkripsi dan dekripsi artinya semakin besar ukuran filenya maka semakin lama pula waktu prosesnya.
2. Faktor – faktor yang berpengaruh terhadap hasil *chipertext* setelah dilakukan proses enkripsi dengan menggunakan *Algoritma Blowfish* dan *TripleDES* antara lain *plaintext* dan kunci. Faktor – faktor tersebut memiliki pengaruh yang berbeda – beda, perubahan yang kecil pada *plaintext* maupun pada kuncinya akan menyebabkan perubahan yang signifikan terhadap *chipertext* yang dihasilkan.
3. Nilai rata – rata *Avalanche Effect* dengan *plaintext* untuk *Blowfish* sebesar 43.638 %, 51.655%, 50.738% dan *TripleDES* 50,887%, 49.304%, 49.361% sedangkan *Avalanche Effect* dengan kunci untuk *Blowfish* sebesar 49.49%, 49.396%, 50.276% dan *TripleDES* 47.91%, 49.813%, 48.104% sehingga kedua algoritma kriptografi tersebut tergolong baik dalam menyandikan data.
4. Algoritma *Blowfish* lebih baik untuk sistem keamanan file dibandingkan algoritma *TripleDES*. Dilihat dari lama waktu enkripsi dan lama waktu dekripsi serta dari nilai avalanche effect, algoritma *Blowfish* lebih baik dibanding algoritma *TripleDES*.

5.2. Saran

1. Dapat dilakukan terhadap pengujian metode Algoritma yang lain seperti Twofish, Rijndael dan lainnya untuk memperoleh hasil data yang lebih bervariasi.
2. Dilakukan analisa metoda avalanche effect yang bukan hanya dengan file teks.
3. Bisa dicoba menggunakan program lain seperti, matlab, java dan lainnya.

DAFTAR PUSTAKA

[1] Aditya, Yogie. (2010*). Studi Pustaka Untuk Steganografi Dengan beberapa Metode,* Prosiding Seminar Nasional Aplikasi Teknologi Informasi Yogyakarta.

[2] Alatas, Putri. (2009). *Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital*. Jakarta : Universitas Gunadarma.

[3] *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish).* http://schneier.com. Diakses pada tanggal 14 Desember 2012

[4] Krisnawati. 2008. *Metode Least Significant Bit (LSB) dan End Of File (EOF) Untuk Menyisipkan Teks ke Dalam Citra Grayscale*. Yogyakarta: UPN Veteran.

[5] Marcel, Jonathan. (2010). *Studi Perbandingan Cipher Blok Algoritma Blowfish Dan Algoritma Camellia*. Bandung: Program Studi Teknik Informatika ITB.

[6] Purwanto, Anggi. (2010). *Implementasi Sistem Keamanan File Menggunakan Algoritma Blowfish Pada Jaringan LAN*. Bandung : Program Studi Teknik Telekomunikasi Institut Teknologi Telkom.

[7] Rizal, Muh. (2012). *Analisa Perbandingan Metode Enkripsi Rijndael dan TripleDes Untuk Pengamanan Data*. Bandung: Program Studi Teknik Telekomunikasi Institut Teknologi Telkom.

[8] *Studi dan Implementasi Algoritma Blowfish Untuk Aplikasi Enkripsi dan Dekripsi File* http:// www.informatika.org Diakses pada tanggal 14 Desember 2012.

[9] Supani, Ahyar. *Sistem keamanan File dan Folder Data Menggunakan algoritma Blowfish denganKunci Simetrik* http://www.cert.or.id/ ~budi/ courses/ el695/projects/report-ahyar.doc. Diakses 17 Desember 2012.

[10] Sutanto, Candra Alim. (2009). *Penggunaan Algoritma Blowfish Dalam Kriptografi*. Bandung: Program Studi Teknik Informatika ITB.

[11] *The Blowfish Encryption Algorithm.* http://www.schneier.com diakses pada tanggal 19 Oktober 2012

[12] Rinaldi Munir, *Kriptografi* , Informatika Bandung, 2006