ANALISA PERBANDINGAN METODE ENKRIPSI RIJNDAEL DAN TRIPLE DES UNTUK PENGAMANAN DATA

Muh. Rizal[1], Indrarini Dyah Irawati[2], Iman Hedi Santoso[3]

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

---

Abstrak

Kriptografi, Enkripsi, Dekripsi, Plaintext, Chipertext, Rijndael, Triple Des, Avalanche Effect by Key, Avalanche Effect by Plaintext

Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan. Pada Tugas Akhir ini akan dibuat suatu aplikasi program tersebut bertujuan untuk menganalisa perfomance perbandingan kinerja dengan cara menghitung waktu proses Enkripsi dan Dekripsi data kemudian dari segi keamanan digunakan dua metode yaitu Avalanche Effect By Plaintext dan Avalanche Effect By Key dengan menggunakan Metode Enkripsi Rijndael dan Triple Des.

Setelah melalui proses perancangan hingga pengambilan beberapa sample dengan menggunakan aplikasi program yang telah dibuat maka dapat ditarik kesimpulan bahwa proses perhitungan waktu Enkripsi dan Dekripsi Rijndael lebih cepat dibandingkan dengan Triple DES, lama waktu prose Enkripsi dan Dekripsi berbanding lurus dengan besarnya file, perubahan kecil pada Plaintext akan akan berpengaruh pada output Chipertextnya, dan perhitungan Avalanche Effect dilakukan dengan dua cara yaitu Avalanche Effect by Plaintext dan Avalanche Effect by Key.

Kata Kunci : Kriptografi, Enkripsi, Dekripsi, Plaintext, Chipertext, Rijndael, Triple Des, Avalanche Effect by Key, Avalanche Effect by Plaintext

---

Abstract

Security has become a major aspect of an information system. A general information only intended for a certain community. It is therefore very important to prevent it from falling to other parties who are not interested. Issues of data security and confidentiality is very important in an organization or individual. Moreover, if the data is located in a network of computers connected with a public network such as internet. Of course, very important data can be viewed or hijacked by unauthorized persons. It's certainly not because we wish we could have the data that is private, because if this is likely to happen possibility damaged the data or can be lost even that will cause huge material losses.

Cryptography is really a study of mathematical techniques related to security aspects of an information system, such as confidentiality, data integrity, authentication, and the absence of denial. At this final project will be an application program aims to analyze the perfomance of comparison by calculating time process the Encryption and Decryption of data in terms of security and then used two methods, namely Avalanche Effect By Plaintext and Avalanche Effect By Key using the method of Rijndael and Triple DES Encryption.

After going through the design process to capture some of the sample by using an application program that has been created it can be concluded that the calculation time Rijndael Encryption and Decryption faster than Triple DES, Long time Encryption and Decryption process is directly proportional to the size of a file, a small change in the plaintext will be an effect on the output ciphertext, and the Avalanche Effect calculations done in two ways by Plaintext Avalanche Effect and Avalanche Effect by Key .

Keywords : Kriptografi, Encryption, Decryption, Plaintext, Chipertext, Rijndael, Triple Des, Avalanche Effect by Key, Avalanche Effect by Plaintext

---

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Kriptografi adalah seni dan ilmu untuk melindungi informasi dari individu yang tidak diinginkan dengan mengubah kedalam yang tidak dikenali oleh pihak yang tidak berwenang , lalu ditransmisikan ditransmisikan [1]. Data kriptografi merupakan data acak yang terdiri dari, teks, gambar,audio, video. Untuk membuat data tidak terbaca,terlihat atau tidak dapat dimengerti selama transmisi disebut Enkripsi. Tujuan utama dari kriptografi adalah menjaga Data dengan cara mengamankan dari pihak yang tidak berwenang, sedangkan proses pembalikan data disebut ke data asli yang sama waktu proses pengiriman disebut Dekripsi.

Pada jurnal *International Journal of Computer and Science and Information Security* dengan judul "A Novel Generic Session Based Bit Level Encryption Technique to Enhance Information Security" dibahas mengenai kemampuan mengamankan berbagai macam data baik itu Audio, Video maupun Text dengan metode Advanche Encryption Standard (AES), Triple DES dan Permutated Chiper Technique (PCT) dengan cara melakukan proses Enkripsi dan Dekripsi data, ketiga metode tersebut termasuk dalam katagori Kriptografi Simetris yang bersifat stream chiper dimana dalam analisa jurnal penulis membandingkan ketiga metode tersebut untuk menghitung waktu proses Enkripsi dan Dekripsi data untuk mengetahui segi perfomansinya, dan dari segi keamanannya menghitung nilai Avalanche Effectnya. Dalam tugas akhir ini penulis juga melakukan hal yang sama dengan membandingkan metode Rijndael dengan metode Triple DES dengan tujuan untuk mendapatkan data yang lebih bervariasi sehingga pada kesimpulannya dapat diketahui metode mana yang lebih unggul dalam segi perfomansi dan keamanannya.

Dalam metode kriptografi terdapat dua proses yaitu proses Enkripsi dan Dekripsi. Metode Algoritma kriptografi yang akan digunakan ialah Algoritma Kriptografi Simetris dan bersifat *stream cipher* sehingga data hasil Enkripsi (Chipertext) mempunyai ukuran yang sama dengan data asli (Plaintext). Teknik

kriptografi simetris dipilih karena diharapkan dengan Algoritma ini proses Enkripsi – Dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan Algoritma kriptografi kunci publik (Asimetris)[2][3].

Untuk menilai tingkat keamanan sebuah Algoritma kriptogarafi dapat menggunakan banyak cara seperti Avalanche Effect, Block Size, Key Size, Mode Of Operation, dan Weak Key. 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. Karena Algoritma Rijndael dan Triple DES beroperasi dalam byte, maka Avalanche Effect cocok untuk mengetahui tingkat keamanan suatu Algoritma kriptografi tersebut[4].

Berdasarkan atas informasi diatas, penulis membuat sebuah aplikasi program dengan menerapkan metode sistem Enkripsi simetris untuk mengamankan data yang dibentuk kedalam Tugas Akhir untuk menyelesaikan studi pada program Sarjana Strata Satu (S1) **Institut Teknologi Telkom** dengan judul "**Analisis Perbandingan Metode Enkripsi Rijndael Dan Triple Des Untuk Pengamanan Data**".

1.2. TUJUAN

Tujuan pada penelitian tugas akhir ini adalah sebagai berikut :

1. Membuat suatu aplikasi software yang dapat mengenkripsi berbagai jenis macam data baik itu berupa Text, Audio dan Video.
2. Menganalisa tingkat keamanan dari Algoritma kriptografi Rijndael dan Triple DES dengan menghitung nilai Avalanche Effectnya.
3. Menganalisa lama waktu proses Enkripsi dan Dekripsi menggunakan Algoritma Rijndael dan Triple DES.

1.3. RUMUSAN MASALAH

Berdasarkan latar belakang masalah diatas, identifikasi masalahnya adalah:

1. Bagaimana membuat suatu aplikasi software yang dapat mengenkripsi berbagai jenis macam data baik itu berupa Text, Audio dan Video.
2. Bagaimana menganalisa tingkat keamanan dari Algoritma kriptografi Rijndael dan Triple DES dengan menghitung nilai Avalanche Effectnya.
3. Bagaimana menghitung lama waktu proses Enkripsi dan Dekripsi menggunakan Algoritma Rijndael dan Triple DES.

1.4. BATASAN MASALAH

Batasan masalah dalam penelitian dan pengembangan tugas akhir ini adalah:

1. Algoritma yang digunakan adalah Algoritma kriptografi AES Rijndael dan Triple DES.
2. Hanya membahas Kriptografi Simetris.
3. Tidak membahas masalah jaringan dan trafiknya.

1.5. METODE PENELITIAN

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

a. Studi literatur

   Studi literatur ini dimaksudkan untuk mempelajari konsep dan teori-teori yang dapat mendukung proses perancangan sistem yang telah dibuat.

b. Perancangan dan realisasi

Meliputi aplikasi dari konsep dan teori yang telah diperoleh. Melakukan pengujian terhadap hasil perancangan yang telah dikerjakan.

c. Pengujian dan analisis implementasi

- Membuat aplikasi program yang dapat melakukan proses Enkripsi dan Dekripsi berbagai macam jenis data dengan menggunakan metode Algoritma kriptografi AES Rijndael dan Triple DES.
- Melakukan analisis cara kerja dalam proses Enkripsi 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 Analisis Kebutuhan dan Pemodelan 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 Pengujian**

   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 Rijndael lebih cepat dibandingkan dengan metode TDES. 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 Kriptografi Rijndael dan TDES antara lain Plaintext dan Key. Faktor – faktor tersebut memiliki pengaruh yang berbeda – beda, perubahan yang kecil pada Plaintext maupun pada Keynya akan menyebabkan perubahan yang signifikan terhadap Chipertext yang dihasilkan.
3. Perhitungan Avalanche Effect dilakukan dengan dua cara pertama memasukkan dua Plaintext yang memiliki perbedaan satu bit dengan dua buah Key yang sama yang disebut “Avalanche Effect By Plaintext” , yang kedua memasukkan dua Key yang berbeda dengan dua Plaintext yang sama yang disebut “Avalanche Effect By Key”. Nilai rata – rata Avalanche Effect By Plaintext untuk Rijndael sebesar 49.93% dan TDES 50.88 % sedangkan Avalanche Effect By Key untuk Rijndael sebesar 49.47 % dan TDES 49.63 % sehingga kedua Algoritma Kriptografi tersebut tergolong baik dalam menyandikan data.

5.2. Saran

1. Dapat dilakukan terhadap pengujian metode Algoritma yang lain untuk memperoleh hasil data yang lebih bervariasi.
2. Dilakukan pengujian Enkripsi dan Dekripsi dengan penyimpanan data menggunakan sistem database untuk menguji sistem keamanan yang lebih lanjut.

DAFTAR PUSTAKA

[1] A.A.Zaidan, B.B.Zaidan, Anas Majeed, "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm", World Academy of Science Engineering and Technology (WASET), Vol.54, ISSN: 2070-3724, P.P 468-479

[2] A.A.Zaidan, B.B.Zaidan, M.M.Abdulrazzaq, R.Z.Raji, andS.M.Mohammed," Implementation Stage for High Securing Cover-File of Hidden Data Using Computation Between Cryptography andSteganography", International Conference on Computer Engineeringand Applications (ICCEA09), Telecom Technology and Applications(TTA), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database,British Library and EI Compendex, Vol.19, Session 6, p.p 482-489.

[3] A.W. Naji, A.A.Zaidan, B.B.Zaidan, Ibrahim A.S.Muhamadi, "NovelApproach for Cover File of Hidden Data in the Unused Area Twowithin EXE File Using Distortion Techniques and AdvanceEncryption Standard.", Proceeding of World Academy of ScienceEngineering and Technology (WASET),Vol.56, ISSN:2070-3724, P.P498-502.

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

[5] Yusuf Kurniawan, *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika, 2004

[6] William Stalling (2006), Cryptography and Network Security: Principles and Practices

[7] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standardsand Technology, U.S. Department of Commerce, November 26, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[8] A.G Konheim, Cryptography : A Primer, John Wiley and sons, 1981