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.