BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama yang berisi informasi sensitif yang hanya diketahui isinya oleh pihak tertentu, sehingga perlu dilakukan penyandian data supaya berapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Di Universitas Muhammadiyah Jember menjelaskan bahwa ilmu yang mempelajari tentang proses pengamanan data adalah kriptografi. Ada banyak algoritma yang digunakan oleh orang untuk mengamankan data tersebut, diantaranya adalah *Algoritma Data Encryption Standard* (DES) dan *Three Data Encryption Standard* (3DES).

DOC adalah sebuah format dokumen yang memungkinkan di dalamnya text, gambar, grafik. DOC merupakan singkatan dari *Document*. Proses pencurian data secara fisik yang masih sering terjadi yaitu mengambil data langsung ke pusat data. Di tahun 2017, terdapat 1.9 milyar kasus pencurian dan kehilangan data sensitif melalui 918 insiden. Jika dibandingkan dengan tahun 2016 di periode yang sama, kasus pelanggaran data di tahun 2017 terdapat kenaikan 13% (https://jakartaurbanhosting.com/kasus-pencurian-data-terbesar-2017/). Keamanan di dalam sebuah data center diperlukan beberapa hal untuk mencegah terjadinya pencurian informasi tersebut. Adapun prosedur keamanan dapat dilakukan untuk mengatasi masalah tersebut biasanya dengan cara menggunakan sistem authentifikasi yang berlapis. Hal ini dimaksudkan agar keamanan dapat berlapis dan juga hanya beberapa user saja yang memiliki *privilledge* khusus yang dapat mengakses data center utama.

Namun seiring dengan teknologi yang semakin berkembang cara mengatasi sistem pencurian tersebut masih belum dapat mengurangi permasalahan. Perlu dilakukan proses perbandingan algoritma yang lebih aman untuk melakukan pengamanan data khususnya data berformat DOC.

Triple Data Encryption Standard (3DES) adalah sistem penyandian berlapis tiga dari DES, proses tersebut menyebabkan ukuran key bertambah dari

56bit menjadi 168bit, tanpa memerlukan perancangan sandi blok (*block chiper)* yang baru.

Dalam kasus ini, peneliti ingin mengimplementasikan pengamanan dokumen dengan metode *Triple Data Encryption Standard* (3DES), dengan judul ***"Penerapan Metode Triple Data Encryption Standard (3DES) Pada File Doc"***

1.2 Rumusan Masalah

Adapun perumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses enkripsi dan deskripsi dengan menggunakan metode 3DES?
2. Bagaimana hasil enkripsi file .doc menggunakan metode 3DES?

1.3 Batasan Masalah

1. Pada skripsi ini tidak membahas mengenai sulitnya cara-cara untuk memecahkan mekanisme penyandian.
2. File teks yang akan digunakan adalah file .doc.
3. Panjang kata sandi minimal 6 karakter.

1.4 Tujuan Penelitian

Adapun tujuan dari penulisan skripsi ini adalah :

1. Untuk mengetahui proses enkripsi dan dekripsi dengan menggunakan metode 3DES.
2. Untuk mengetahui hasil enkripsi file .doc menggunakan metode 3DES.

1.5 Manfaat Penelitian

Sebagai bahan refrensi mengenai cara penyandian kata kunci dengan metode 3DES.