BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dengan semakin berkembangnya teknologi, informasi menjadi aspek penting yang kerahasiaan dan keamanannya harus terjaga. Tidak sedikit pihak yang ingin mendapatkan informasi yang bersifat rahasia karena dapat memberikan keuntungan bagi pihak terkait. Informasi merupakan suatu hal yang sangat berharga yang bisa dijadikan senjata untuk menjatuhkan pihak-pihak yang terkait seperti pelaku usaha yang dapat menggunakan data informasi dari perusahaan saingannya untuk mendapatkan keuntungan ataupun menjatukan saingannya dengan informasi yang di dapat. Untuk mengatasi itu semua diperlukan suatu cara untuk mengamankan data dan informasi tersebut ke dalam bentuk data dan informasi yang tidak dapat dimengerti oleh pihak lain, yaitu dengan cara penyandian, salah satu bidang ilmu untuk menjaga keamanan data adalah kriptografi. Dengan adanya kriptografi dapat membuat data menjadi lebih aman, informasi yang di anggap rahasia dapat dirubah menjadi sebuah data yang tidak dikenali oleh pihak yang tidak berhak atas informasi tersebut. Banyak jenis algoritma kriptografi di zaman sekarang ini, diantaranya adalah algoritma *Triple* DES *(Data Encrytion Standart).*

Algortima *Triple DES* merupakan pengembangan algoritma DES yang beroperasi pada ukuran blok 64 bit. DES mengenkripsi 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci, sedangkan algoritma *Triple* DES menggunakan 3 kunci yang masing-masing berjumlah 56-bit dengan asumsi total panjang kuncinya 168-bit. Algoritma *Triple* DES dinilai lebih aman dibanding algoritma DES karena panjangnya kunci yang digunakan.

Algortima *Triple* DES merupakan jenis algoritma simetris yang menggunakan kunci enkripsi dan kunci dekripsi yang sama dalam proses penyandiannya.

Sebelumnya telah dilakukan beberapa penelitian terdahulu yang saling berkaitan, di antaranya penelitian[1] yang berjudul “Analisis Dan Implementasi

Enkripsi Dan Dekripsi Ganda Kombinasi Algoritma Blowfish dan Algoritma Triple DES untuk Sms pada Smartphone Android*"*. Penelitian berikutnya dari [2] dengan judul "Implementasi Algoritma Triple-Des (3des) dalam Pengamanan ID Tag Rfid Berbasis Client Server". Penelitian yang ketiga dari[3] dengan judul "Penerapan Aplikasi Pengamanan Data/File Dengan Metode Enkripsi dan Dekripsi Algoritma 3DES Dalam Jaringan Lokal Area". penelitian selanjutnya dari[4] dengan judul *"*Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standart(DES)*"*. penelitian lainnya juga dilakukan oleh[5] dengan judul "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File". Dan pelenitian selanjutnya dilakukan oleh[6] dengan judul "Penerapan Algoritma AES dan Konversi SMS Ke Dalam Bahasa KHEK Pada Aplikasi Enkripsi Berbasis Mobile Application".

Berdasarkan latar belakang di atas, pada penelitian ini penulis akan membangun Aplikasi yang berguna untuk mengamankan suatu data yang akan diimplementasikan dalam penelitian berjudul **"Penerapan Algoritma Triple DES Pada Aplikasi Kriptografi Untuk Meningkatkan Keamanan Data".**

1.2 RUMUSAN MASALAH

Dalam penerapan algoritma *Triple DES* pada aplikasi kriptografi untuk meningkatkan keamanan data dapat dirumuskan masalah sebagai berikut :

1. Bagaimana merancang dan membangun sebuah aplikasi kriptografi untuk mengamankan data menggunakan algoritma *Triple DES*?
2. Bagaimana penerapan algoritma *Triple DES* pada aplikasi kriptografi?
3. Bagaimana proses enkripsi dan dekripsi data menggunakan algoritma *Triple DES*?

1.3 BATASAN MASALAH

Untuk membantu mempermudah pembuatan aplikasi kriptografi untuk meningkatkan keamanan data menggunakan algoritma *Triple DES* ini agar tidak terlalu luas, peneliti membatasi masalah yang akan dibahas sebagai berikut :

1. Aplikasi ini dibangun menggunakan bahasa pemrograman Microsoft Visual Studio 2008 Versi 9.0.
2. Aplikasi ini menggunakan Algoritma *Triple DES*.
3. Aplikasi ini dibuat berbasis *dekstop*.
4. Tidak membahas penyerangan pada saat pengiriman data melalui jaringan.
5. Aplikasi ini hanya dapat dekripsi data yang telah di enkripsi dengan kunci yang sama.
6. Aplikasi ini mengubah ekstensi data yang dienkripsi menjadi *.usb*
7. Tidak membahas kecepatan proses enkripsi dan dekripsi data.

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan dari penelitian ini adalah :

1. Merancang dan membangun suatu aplikasi kriptografi yang berfungsi untuk mengamankan data dalam upaya melindungi dari orang yang tidak berhak dengan menggunakan algoritma *Triple DES.*
2. Mengetahui proses algortima *Triple DES* pada aplikasi kriptografi.
3. Mengetahui proses enkripsi dan dekripsi data menggunakan algoritma *Triple DES.*

1.4.2 Manfaat :

1. Aplikasi kriptografi ini diharapkan mampu mengamankan data dari user/orang yang tidak berhak atas data tersebut.
2. Aplikasi kriptografi ini diharapkan mampu mengamankan berbagai jenis data.

1.5 SISTEMATIKA PENULISAN

Untuk mempermudah pembahasan, keseluruhan perancangan sistem aplikasi ini dibagi menjadi lima bab dengan pokok pikiran dari sub-sub bab sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang penulisan laporan, rumusan masalah, batasan masalah, tujuan serta manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini penulis akan menjelaskan berbagai teori yang berkaitan dengan topik penelitian yang dilakukan serta teori pendukung sesuai topik penelitian.

BAB III METODOLOGI PENELITIAN

Pada bab ini penulis akan membahas model pengembangan perangkat lunak, *tools* pengembangan sistem, serta algoritma yang digunakan.

BAB IV PEMBAHASAN DAN HASIL

Pada bab ini penulis akan membahas mengenai analisis permasalahan, analisis solusi permasalahan, analisis kebutuhan sistem, algoritma, perancangan sistem dan perancangan layar pada sistem, serta hasil dari penelitian.

BAB V PENUTUP

Pada bab ini penulis menarik kesimpulan dari keseluruhan bab, memberi beberapa saran yang diharapkan dapat bermanfaat dalam pengembangan aplikasi.