BAB I

PENDAHULUAN

1.1. Latar Belakang

Sekarang ini pertukaran informasi sudah semakin berkembang pesat, teknologi informasi juga telah terbukti mendorong kinerja pada berbagai bidang contoh nya di bidang keamanan, Bidang keamanan sendiri digunakan untuk mengamankan suatu data. Data merupakan bentuk jamak dari *datum* yang berarti fakta atau bagian dari peristiwa yang memiliki arti yang dihubungkan dengan, simbol, gambar, angka, huruf, yang menunjukkan berbagai ide, objek dan lain-lain. (Bangun & Setiawan, 2016)

Data memiliki berbagai kategori, ada yang sifatnya rahasia maupun tidak rahasia, data yang bersifat rahasia memiliki informasi yang didalamnya sangat dibutuhkan oleh pemilik, sehingga data tersebut perlu diamankan agar tidak disalah gunakan oleh orang yang tidak bertanggung jawab. (Gunawan, 2018)

Berbagai cara dilakukan untuk mengamankan data atau pesan tersebut. Salah satu acara untuk mengamankan data atau informasi tersebut dengan Kriptologi. Kriptografi merupakan ilmu yang memahami tentang pengamanan (kerahasian) tulisan. Karena itu, untuk mengamankan data atau informasi dibutuh suatu cara yang mampu mengatasi masalah keamanan data. Kriptografi sendiri terdiri dari 2 bagian, yaitu kriptografi modern dan kriptografi klasik. Secara teknik algoritma kriptografi di bagi menjadi dua teknik yakni teknik substitusi dan teknik transposisi. (Meko, 2018)

Teknik kriptografi dipercaya dapat menangani masalah keamanan data atau informasi, karena selain menggunakan bahasa pemrograman komputer, kriptografi juga menggunakan rumus-rumus matematika, mulai dari rumus yang sederhana sampai dengan rumus yang kompleks. Dalam kriptografi

terdapat dua konsep, yaitu dekripsi dan enkripsi. Enkripsi merupakan proses dimana data atau informasi dirubah menjadi bentuk yang tidak dikenali / samar sebagai informasi awalnya dengan menggunakan metode tertentu. Sedangkan dekripsi adalah mengubah kembali bentuk yang tidak dikenali menjadi data awal. (Santoso & AlHadi, 2017)

Algoritma yang digunakan dalam pengamanan data atau informasi pun beragam jenisnya, seperti *Caesar,* Abjad Majemuk, *DES*, *IDEA, RSA* dan lain sebagainya. Pada penelitian ini akan dilakukan perbandingan kriptografi dengan metode *RSA* dan *DES* untuk keamanan data.

Berdasarkan uraian permasalahan di atas maka penulis menggunakan bahasa pemrograman java sebagai bahasa pemrograman yang digunakan, untuk itu penulis mengambil judul "PERBANDINGAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA *DATA ENCRYPTION STANDART (DES)* DAN ALGORITMA *RIVEST SHAMIR ADLEMAN (RSA)* UNTUK KEAMANAN DATA" dalam penyusunan proposal skripsi ini.

Dengan studi tentang kriptografi ini diharapkan bisa mengerti perbandingan penggunaan kedua teknik diatas.

1.2. Rumusan Masalah

Permasalahan yang dihadapi dan diharapkan dapat diselesaikan melalui penelitian ini adalah:

1. Bagaimana membandingkan Algoritma DES dan RSA dalam mengamankan data?
2. Bagaimana kita mengetahui kualitas dari algoritma DES dan RSA ?
3. Bagaimana merancang perangkat lunak keamanan data teks agar aman ?

1.3. Tujuan Penelitian

Hasil penelitian ini diharapkan bisa menghasilkan aplikasi yang dapat mengamankan data dengan baik. Tujuan dari penulisan skripsi ini adalah:

1. Untuk membandingkan algoritma DES dan RSA agar bisa mengetahui kemampuan dan perbedaan kedua algoritma yang dilengkapi informasi ukuran data sebelum dan sesudah di enkripsi dalam menambah informasi dan mengamankan data mengenai perhitungan algoritma DES dan RSA dalam dekripsi dan enkripsi plaintext serta menampilkan proses perhitungan manualnya..

2.Mengetahui sejauh mana cara kerja algoritma DES dan RSA

3.Dengan cara mengukur sejauh mana kualitas keamanan dan menggunakan metode DES dan RSA.

1.4. Manfaat Penelitian

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Bagi peneliti lain: menambah ilmu pengetahuan di bidang kriptografi, terutama mengenai perbandingan metode Algoritma , dan dapat menciptakan algoritma kriptografi yang lebih baik dan optimal.

2. Bagi pengguna program aplikasi: menambah ilmu pengetahuan tentang proses keamanan data..

3. Bagi penulis: menambah ilmu pengetahuan di bidang kriptografi dan keamanan, serta matematika dan teknologi informasi.

1.5. Batasan Masalah

Adapun batasan agar perancangan pengamanan data ini fokus, tidak terlalu luas cakupannya maka diperlukan batasan masalah yang akan diambil. Batasan masalah yang akan diambil adalah:

1 Pada penelitian ini hanya bisa mendekripsi dan mengenkripsi data yang berupa tulisan atau teks, bukan gambar maupun suara.
2 Perancangan sistem pengamanan data menggunakan bahasa Pemrograman java NetBeans.
3 Algoritma yang digunakan hanya DES dan RSA.

1.6. Sistematika Penulisan

Dalam skripsi ini, pembahasan terdiri dari lima bab, yang secara singkat diuraikan sebagai berikut :

BAB I PENDAHULUAN

Berisi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, sistematika penulisan. Pada bagian latar belakang masalah menjelaskan alasan penulis melakukan penelitian, awal dari masalah dan pentingnya dilakukan penelitian. Masalah yang terjadi fokus dari penelitian di jelaskan pada bagian perumusan masalah.

BAB II Tinjauan Pustaka

Bab ini berisi tentang landasan teori dan tinjauan pustaka yang menjabarkan berbagai teori konsep dan prinsip utama yang terkait dengan judul yang di ambil penulis.

BAB III Metodoligi Penelitian

Berisi tentang metodologi penelitian yang akan diimplementasikan dalam pembahasan atau analisis dari penelitian yang dilakukan. Ditampilkan dalam bentuk daftar, tabel, grafik, foto atau bentuk lainnya. Pembahasan hasil yang diperoleh berupa penjelasan teoritas. Dalam hal ini peneliti menggunakan metode penelitian observasi, dokumentasi dan wawancara.

BAB IV Hasil dan Pembahasan

Bab ini membahas tentang hasil pengujian alat dan sejauh mana tingkat keakuratan alat tersebut.

BAB V Penutup

Bab ini berisi tentang kesimpulan dan saran dari hasil pembahasan analisis tentang perbandingan kriptografi.