BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi dan komunikasi tumbuh dengan cepat, sehingga mengubah sistem komunikasi analog menjadi digital. Seiring dengan kemajuan sosial ekonomi masyarakat menuntut mobilitas yang semakin tinggi. Kemudian dilandasi dengan adanya kendala dalam pengembangan sistem komunikasi jaringan kabel akibat kondisi alam, maka dikembangkan teknologi *smartphone* atau yang disebut dengan telepon pintar.

Chatting adalah aktivitas berkomunikasi yang dilakukan oleh dua orang atau lebih dengan memanfaatkan aplikasi *chatting* dan jaringan internet. Aplikasi *chatting* saat ini sudah sangat maju. Tidak hanya mengirim pesan teks saja, aktivitas *chatting* sekarang ini juga bisa mengirimkan emoticon, pesan suara, bahkan video. "*Chatting*" merupakan salah fitur dari kecanggihan teknologi informasi saat ini. Mulai dari anak kecil hingga orang dewasa saat ini sudah familiar dengan istilah *chatting*. Singkatnya, pengertian *chatting* adalah suatu program yang melibatkan koneksi internet untuk saling bertukar pesan antar satu orang dengan orang lain. *Chatting* adalah bentuk komunikasi yang paling efektif dan efisien sata ini. Sewaktu proses pengiriman *chat* sangat besar kemungkinan celah keamanan, dimana pesan yang dikirim dapat disadap atau disusupi oleh pihak-pihak yang tidak diinginkan. Salah satu upaya pengamanan pesan yang dapa dilakukan

Adalah dengan menggunakan kriptografi. Permasalahan yang terjadi pada saat melakukan penelitian yaitu masih lemahnya sistem keamanan data terutama dalam pengamanan pesan *chat* dan berkembangnya tindakan penyalahgunaan informasi sehingga diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik agar kerahasiaan pesan terjaga maka implementasi teknik kriptografi simetrik sangat cocok untuk memenuhi kebutuhan keamanan pesan *chat*, seperti algoritma pertukaran kunci *Diffie Hellman* pada algoritma *data encryption standard (DES)*. Algoritma *Diffie Hellman* memiliki suatu kunci simetri untuk melakukan enkripsi dan dekripsi. Dalam pendistribusiannya pertukaran kunci simetris yang tidak mempunyai trafik pesan yang tinggi yaitu menggunakan algoritma pertukaran kunci *Diffie Hellman*. Algoritma dengan protokol *Diffie Hellman* atau *Diffie Hellman key exchange* yang berguna untuk mempertukarkan kunci sesi (simetri). (Dyas Yudi Priyanggodo, 2018).

Berdasarkan masalah yang sudah diuraikan tersebut maka penulis ingin membuat suatu aplikasi pengamanan pesan berbasis android untuk menjaga keamanan pesan chat agar tidak dapat dibaca oleh pihak yang tidak diinginkan maka diperlukan suatu sistem kriptografi. Dalam menemukan suatu sistem kriptografi yang mampu mengamankan pesan chat berbasis android yang nantinya akan menjadi sebuah akan menjadi sebuah judul skripsi yang berjudul **“APLIKASI ENKRIPSI DAN DEKRIPSI PESAN DENGAN PERTUKARAN KUNCI DIFFIE HELLMAN PADA ALGORITMA DATA ENCRYPTION STANDARD (DES)".**

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat diberikan untuk penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah yang terdapat pada penelitian ini adalah sebagai berikut :

1. Masih lemahnya sistem keamanan data terutama dalam pengamanan pesan *chatting* .
2. Berkembangnya tindakan penyalahgunaan informasi sehingga diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik agar kerahasiaan pesan *chatting* terjaga.
3. Kurangnya proteksi terhadap pesan yang sudah di enkripsi.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana cara merancang sebuah aplikasi pengamanan pesan menggunakan algoritma pertukaran kunci *Diffie Hellman* pada algoritma *data encryption standard (DES*) untuk meningkatkan keamanan data pada pesan *chatting* ?
2. Bagaimana mengimplementasikan algoritma pertukaran kunci *Diffie Hellman* pada algoritma *data encryption standard (DES*) agar menjadi sebuah teknik pengamanan pesan *chatting*?

3. Bagaimana memahami cara kerja metode algoritma pertukaran kunci *diffie hellman* pada algoritma *data encryption standard* (DES) untuk meningkatkan keamanan pada proses enkripsi dan deskripsi?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

1. Proses enkripsi dan deskripsi hanya untuk untuk mengamankan pesan berupa teks.
2. Kapasitas pesan yang di enkripsi maksimal sebanyak 256 karakter .
3. Aplikasi ini dirancang menggunakan perangkat lunak *android studio* dan akan digunakan pada *smartphone* android.
4. Aplikasi ini menggunakan algoritma Data Encryption Standard (DES) untuk proses enkrisi dan deskripsi dan metode Diffie Hellman untuk mengamankan (mengunci) pesan yang telah di enkripsi.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Untuk mengetahui dan menerapkan metode algoritma pertukaran kunci *diffie hellman* pada algoritma *data encryption standard* (DES) untuk pengamanan pesan.

2. Untuk mengetahui proses enkripsi dan dekripsi pesan dengan menggunakan algoritma pertukaran kunci *diffie hellman* pada algoritma *data encryption standard* (DES).
3. Untuk keamanan dan kerahasiaan pesan agar tidak mudah untuk diakses pihak-pihak yang tidak berwenang.

I.3.2. Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan deskripsi di dalam pengamanan dan kerahasiaan keamanan pesan menggunakan algoritma pertukaran kunci *diffie hellman* pada algoritma *data encryption standard* (DES).
2. Dengan adanya sistem ini, proses pengamanan pesan diharapkan lebih aman dan terhindar dari pencurian data.
3. Sebagai dasar atau referensi dalam penerapan algoritma pertukaran kunci *diffie hellman* pada algoritma *data encryption standard* (DES).

I.4. Kontribusi Penelitian

1. Penelitian ini dapat menjadi referensi terbaru bagi peneliti berikutnya.
2. Penelitian ini dapat menjadi aplikasi yang bermanfaat dalam mengamankan pesan *chat.*
3. Penelitian ini dapat berkembang mengamankan pada aplikasi lainnya bukan hanya mengamankan *chat* saja.

I.5. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan dan saran.