BAB I

PENDAHULUAN

I.1. Latar Belakang

Dalam perkembangan teknologi komputer dan jaringan komputer saat ini, khususnya komunikasi pesan teks lewat *chatting* banyak hal yang harus diperhatikan khususnya keamanannya. *Chatting* merupakan kegiatan saling bertukar pesan maupun informasi melalui jaringan komputer. Namun apabila pesan yang dikirim masih dalam bentuk pesan asli (*plaintext*), tentu pesan tersebut ada kemungkinan untuk disadap oleh pihak-pihak yang tidak berhak tanpa ada kesulitan sekalipun untuk membaca isi dari pesan atau informasi tersebut. Apalagi jika saluran komunikasi yang digunakan untuk *chatting* kurang aman, tentu akan mempermudah pihak yang tidak bertanggung jawab tersebut untuk memonitor seluruh isi percakapan yang terjadi di saluran komunikasi tersebut.

Oleh karena itu timbul suatu gagasan yang mengacu pada permasalahan-permasalahan tersebut, yakni untuk membuat suatu aplikasi keamanan pesan *chatting* yang dapat melindungi isi pesan dengan cara menyandikan pesan tersebut sehingga sulit untuk dibaca maupun dipahami oleh pihak-pihak yang tidak berhak atas pesan tersebut.

Dalam hal ini penulis mencoba menerapkan algoritma *Blowfish* di dalam aplikasi *chatting* sebagai pengamannya untuk menjaga privasi pengguna. Algoritma *Blowfish* sendiri merupakan algoritma kriptografi simetris sehingga menurut penulis sangat sesuai digunakan sebagai pengaman aplikasi yang

melibatkan banyak pihak seperti aplikasi *chatting*. karena selain algoritma ini cepat dalam mengenkripsi maupun mendekripsi, kunci yang digunakan oleh kedua belah pihak juga sama sehingga tidak perlu penyesuaian kunci pada tiap orang yang berbeda seperti pada algoritma asimetris. Hal ini diharapkan mampu untuk melindungi isi pesan dari pihak-pihak yang tidak berhak, sehingga para pengguna aplikasi ini tidak perlu harus khawatir jika isi dari pesan-pesan tersebut jatuh ketangan pihak-pihak yang tidak berhak atas pesan tersebut. Berdasarkan latar belakang di atas maka penulis akan mengangkat sebuah judul **"Perancangan Keamanan *Chatting* Berbasis *Client Server* Menggunakan Metode *Blowfish* Pada *Android*".**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun beberapa permasalahan yang penulis peroleh dalam penelitian ini adalah sebagai berikut:

1. Merancang sebuah aplikasi *chatting* untuk perangkat *Android*.
2. Membangun keamanan dalam sebuah aplikasi *chatting*.
3. Menerapkan metode *Blowfish* pada sebuah aplikasi *chatting*.

I.2.2. Rumusan Masalah

Berikut ini beberapa rumusan masalah tentang penelitian ini yang akan dicari penyelesaiannya antara lain:

1. Bagaimana cara merancang sebuah aplikasi *chatting* untuk perangkat *Android*?
2. Bagaimana cara membangun keamanan dalam sebuah aplikasi *chatting?*
3. Bagaimana cara menerapkan algoritma *Blowfish* pada sebuah aplikasi *chatting?*

I.2.3. Batasan Masalah

Untuk menghindari kesimpangsiuran dalam penulisan skripsi ini serta karena keterbatasan waktu, biaya dan tenaga penulis, maka dari itu penulis membatasi masalah yang akan dibahas dalam skripsi ini diantaranya:

1. Membahas tentang proses enkripsi dan dekripsi pesan teks pada aplikasi *chatting* yang akan dirancang.
2. Aplikasi yang dibuat hanya digunakan untuk mengirimkan pesan teks, bukan untuk mengirimkan gambar, suara, dan lain-lain.
3. Analisa penelitian dengan menggunakan akses *client server* melalui koneksi *wifi* sebagai uji coba sistem.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Membuat aplikasi *chatting* untuk perangkat *Android*.
2. Membuat aplikasi *chatting* yang dapat terjamin keamanannya.
3. Menerapkan algoritma *Blowfish* di dalam aplikasi *chatting* tersebut.

I.3.2. Manfaat

Adapun manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Meningkatkan keamanan pada aplikasi *chatting* agar dapat menghindari kekhawatiran bagi pengguna terhadap informasi di dalamnya akan penyadapan yang dilakukan oleh pihak ketiga.
2. Memberi kenyamanan bagi pengguna untuk saling bertukar pesan/informasi rahasia melalui jaringan komputer.

3. Sebagai sarana pengembangan ilmu pengetahuan khususnya dalam bidang ilmu Kriptografi.

I.4. Metodologi Penelitian

Dalam penulisan laporan penelitian ini, penulis menggunakan metode penyelesaian masalah sebagai berikut :

1. Studi Kepustakaan *(Library Research)*

Penulis melakukan studi pustaka untuk memperoleh data-data yang berhubungan dengan penulisan skripsi dari berbagai sumber yang ada, serta teori yang berkaitan dengan judul penulis.

2. Studi *Internet (Internet Research)*

Penulis melakukan studi *internet* untuk memperoleh jurnal-jurnal yang berkaitan dengan judul penulis sebagai tinjauan pustaka untuk mendukung data-data yang diperoleh dari objek penelitian penulis.

I.5. Keaslian Penelitian

Menurut sepengetahuan penulis, penelitian tentang "Perancangan Keamanan *Chatting* Berbasis *Client Server* Menggunakan Metode *Blowfish* Pada *Android*" belum pernah dilakukan, akan tetapi penulis menemui beberapa karya tulis yang menggunakan metode yang sama yaitu metode *Blowfish,* di antaranya yang berjudul "Studi Implementasi Algoritma *Blowfish* Untuk Enkripsi *Email*" dan "Aplikasi Kriptografi *File* Menggunakan Algoritma *Blowfish*". Untuk lebih jelasnya dapat dilihat pada Tabel I.1.

Tabel I.1. Keaslian Penelitian

No.	Peneliti	Judul Penelitian	Variabel	Hasil Penelitian
1.	1. Chumaidi Rahman. 2. Isbat Uzzin Nadhori. 3. Kholid Fathoni.	Studi Dan Implementasi Algoritma Blowfish Untuk Enkripsi Email.	1. Algoritma Blowfish. 2. Email Server dan Client.	1. Cepat. Blowfish dirancang agar dapat mengenkripsikan data pada mikroprosesor 32 bit dengan kecepatan 26 clock cycles per byte. 2. Kompak. Blowfish dirancang agar dapat berjalan dengan penggunaan memori kurang dari 5kB.
2.	1. Suriski Sitinjak. 2. Yuli Fauziah. 3. Juwairiah	Aplikasi Kriptografi File Menggunakan Algoritma Blowfish.	1. Algoritma Blowfish. 2. File-file terkait.	1. Kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file. 3. Semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi. 4. Terjadi penambahan byte pada file hasil enkripsi, namun ketika file enkripsi dikembalikan(didekripsi) ukuran file akan kembali seperti ukuran file plainteksnya.

Berdasarkan dari kedua judul tersebut penulis akan mencoba untuk membandingkannya dengan yang akan dibahas oleh penulis. Jika dilihat dari segi metode yang digunakan tidak ada perbedaan dengan yang akan dibahas penulis, akan tetapi dari segi penerapannya terdapat perbedaan yang cukup signifikan. Pada objek penelitian yang akan dibahas oleh penulis, penulis menerapkan metode *Blowfish* di dalam aplikasi *chatting* untuk platform *Android* sehingga membutuhkan proses enkripsi dan dekripsi yang cepat karena pada umumnya aplikasi *chatting* bersifat *realtime*.

I.6. Sistematika Penulisan

Langkah dan tahapan yang ditempuh dalam menyelesaikan penulisan ini adalah :

BAB I PENDAHULUAN

Dalam BAB ini di bahas mengenai Latar Belakang Masalah, Ruang Lingkup Permasalahan, Tujuan dan Manfaat Penelitian, Metodologi yang digunakan serta Sistematika Penulisan ini sendiri.

BAB II LANDASAN TEORI

Pada BAB ini dijelaskan teori-teori penujang yang digunakan sebagai dasar dalam proses perancangan dan pembuatan aplikasi, serta membahas tentang pengertian Kriptografi, Algoritma *Blowfish*, dan Algoritma Simetris.

BAB III ANALISIS DAN DESAIN SISTEM

Pada BAB ini membahas tentang cara kerja dari metode yang digunakan dalam proses pemecahan masalah, dalam hal ini penulis menerapkan metode *Blowfish* untuk sistem baru yang lebih baik.

BAB IV HASIL DAN UJI COBA

Pada BAB ini berisikan tentang tampilan hasil, pembahasan, kelebihan dan kekurangan dari sistem yang dirancang.

BAB V KESIMPULAN DAN SARAN

BAB ini merupakan penutup dari penulis laporan Skripsi ini yang berisikan kesimpulan atas hasil analisa dan perancangan serta berisikan saran-saran.