

BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan kemajuan teknologi informasi telah semakin berkembang dengan banyak kemudahan yang didapat oleh masyarakat. Pengamanan terhadap kerahasiaan sebuah informasi dalam proses pertukaran data. Dalam hal ini komunikasi atau pertukaran data yang menggunakan layanan media jaringan local atau sering disebut LAN (*local area network*) maupun WLAN (*wireless local area network*). Dengan menggunakan media jaringan lokal, pengguna dapat berbagi atau bertukar data antara satu pengguna dengan pengguna lain dalam satu jaringan yang terhubung. Di dalam dunia informatika dikenal dengan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau lebih dikenal dengan istilah Kriptografi.

Berbagi dan transfer *document* antar pengguna telah dapat mudah dilakukan dengan hanya terhubung pada jaringan *Wifi* melalui perangkat *mobile phone Android*. Pengamanan dokumen atau data yang bersifat penting dan mengatasi hal – hal penyalahgunaan diperlukan sebuah cara untuk mengamankan suatu data atau informasi dengan menggunakan teknik kriptografi. Saat ini sudah banyak berkembang algoritma kriptografi yang mendukung untuk mengamankan suatu data atau informasi yang ada dari orang atau pihak yang tidak berhak untuk mengakses data atau informasi tersebut.

RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi. Algoritma kriptografi *Rivest Code 4 (RC4)* merupakan salah satu algoritma kunci simetris dibuat oleh *RSA Data Security Inc (RSADSI)* yang berbentuk stream *chipper*. Algoritma ini ditemukan pada tahun 1987 oleh *Ronald Rivest* dan menjadi symbol keamanan *RSA* (merupakan singkatan dari tiga nama penemu : *Rivest, Shamir, dan Adleman*).

Penulis mencoba untuk membangun sebuah aplikasi yang dapat mengamankan data *file* teks dengan algoritma kriptografi *Rivest's Chipper 4*. Penelitian untuk perancangan ini diberi judul "Perancangan dan Implementasi Pengamanan Data Teks Dalam Proses Transfer File Pada Perangkat *Android* Dengan Algoritma *RC4*".

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Penulis mengidentifikasi beberapa masalah yang ditemukan dalam penelitian ini sebagai berikut :

1. Mudahnya penyalahgunaan *file* atau dokumen oleh pengguna yang tidak berhak karena proses transfer *file* tidak memiliki pengamanan data.
2. Masih sedikitnya penerapan sistem pengamanan data di dalam proses transfer *file* melalui jaringan *Wifi*.
3. Dibutuhkannya aplikasi yang mendukung pengamanan data *file* teks yang diimplementasikan dalam proses transfer pada *mobile phone Android*.

I.2.2. Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana membangun aplikasi pengamanan data teks dalam proses *file* data *android* dengan algoritma *RC4* pada perangkat *mobile phone android* ?
2. Bagaimana proses yang terjadi dalam aplikasi pengamanan data teks dengan algoritma *RC4*?

I.2.3. Batasan Masalah

Dalam penulisan skripsi ini penulis membatasi permasalahan agar pembahasan tidak rancu dari penelitian, yaitu sebagai berikut :

1. Aplikasi yang direncanakan adalah aplikasi yang dapat melakukan pengamanan data *file* teks dalam transfer *file*.
2. Uji coba dan perancangan menggunakan koneksi jaringan *Wifi*.
3. Implementasi pengamanan data *file* menggunakan algoritma *Rivest's Chipper*
- 4.
4. Pemrograman menggunakan bahasa pemrograman *Java*.
5. Perangkat yang digunakan adalah *mobile phone* dengan system operasi *Android*.

I.3. Tujuan dan Manfaat Penelitian

I.3.1. Tujuan Penelitian

Adapun tujuan dari penelitian penulis ini adalah :

1. Untuk menerapkan teknik kriptografi dalam pengamanan data *file* teks untuk transfer *file* melalui jaringan *Wifi*.
2. Untuk menyediakan aplikasi yang dapat mengamankan *file* teks dengan transfer data melalui perangkat *mobile phone Android*.
3. Untuk mengimplementasikan sebuah teknik pengamanan data dengan algoritma kriptografi *Rivest's Chipper 4* dan pengembangan untuk *mobile phone Android*.

I.3.2. Manfaat Penelitian

Adapun manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Memberikan kemudahan kepada pengguna sebuah aplikasi untuk pengamanan data *file* teks dalam transfer *file* melalui jaringan *Wifi*.
2. Menyajikan aplikasi yang dikhususkan untuk mengamankan data *file* teks Dengan kemudahan enkripsi dan dekripsi dengan algoritma *Rivest's Chipper 4* pada perangkat *mobile phone Android*.

I.4. Metodologi Penelitian

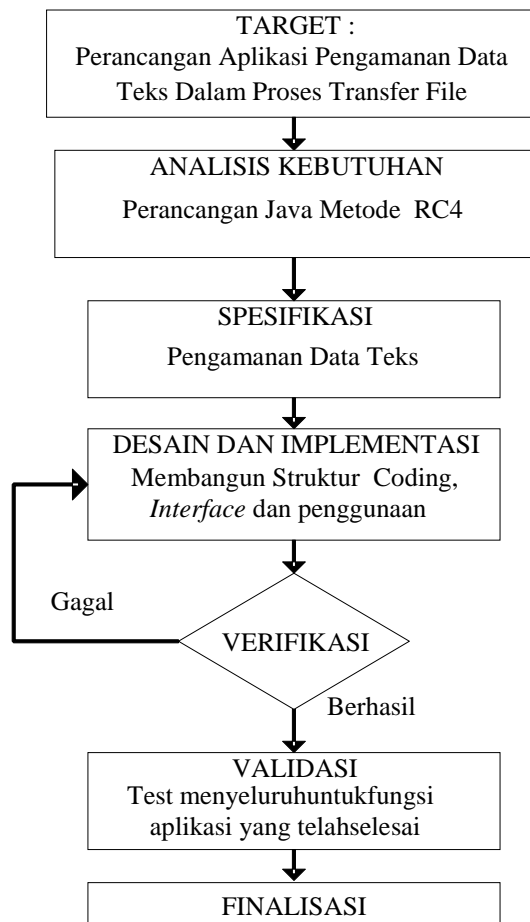
I.4.1. Teknik Pengumpulan Data

Adapun teknik-teknik pengumpulan data yang dilakukan penulisan adalah sebagai berikut :

1. Penelitian ini bersifat teoritis dengan cara memperoleh informasi dalam buku bacaan, jurnal, artikel yang berhubungan dengan masalah yang akan dibahas yang berasal dari akademik atau pun dari luar akademik, terutama yang berkaitan dengan prosedur, implementasi bahasa pemrograman *Java*

dalam perancangan pengamanan Data Teks Dalam Proses Transfer *File* pada perangkat *Android* Dengan Algoritma *RC4*.

2. Adapun prosedur perancangan aplikasi yang dibuat terdiri dari beberapa tahapan, yaitu sebagai berikut:



Gambar I.1. Prosedur Perancangan

a. Target

Perancangan dan Implementasi Pengamanan Data Teks Dalam Proses Transfer *File* Pada Perangkat *Android* Dengan Algoritma *RC4*.

b. Analisis Kebutuhan

Melakukan analisa terhadap kebutuhan yang akan digunakan dalam aplikasi, algoritma yang digunakan serta konsep jaringan pada aplikasi.

c. Spesifikasi dan Desain.

Sistem yang akan penulis buat nantinya akan diuji coba menggunakan *software* dan *hardware*.

d. Implementasi dan Verifikasi.

Selanjutnya dilakukan pembuatan aplikasi dengan memanfaatkan masing-masing komponen. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik. Bila ada kesalahan atau kekurangan dapat diperbaiki.

e. Validasi

Selanjutnya dilakukan pengujian aplikasi secara menyeluruh. Setelah melewati tahap validasi dan sistem telah berjalan dengan baik sesuai dengan kebutuhan dan target dari aplikasi yang dirancang.

f. Finalisasi

Proses akhir dari keseluruhan adalah aplikasi hasil perancangan akan dinyatakan *valid* atau sesuai apabila proses kompresi data dan dekompresi yang dilakukan oleh aplikasi sudah sesuai dengan algoritma yang diterapkan.

I.5. Keaslian Penelitian

Setiap penelitian yang dilakukan memiliki bukti keaslian, dimana keaslian tersebut juga dibandingkan dengan penelitian-penelitian yang akan dirancang. Untuk lebih jelasnya perbandingan-perbandingan tersebut dapat dilihat pada tabel I.1. sebagai berikut.

Tabel I.1. Keaslian Penelitian

No	Peneliti	Judul	Hasil
1	Fricles Ariwisanto Sianturi (2013)	Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard (AES)	Teknik yang dilakukan dalam pengamanan data teks ini yaitu dengan cara menerapkan metode AES kedalamnya yang bias mengubah data teks asli kedalam teks rahasia. Megubah data yang ingin diamankan kedalam bilangan hexa baik plainteks dan kuncinya dengan menggunakan tabel ASCII, kemudian dilakukan dengan proses enkripsi dan deskripsi.
2	Gede Andika Putra, Made Widhi Wirawan (2012)	Sistem pengamanan data sidik jari menggunakan algoritma aes pada Sistem kependudukan berbasis <i>radio frequency dentification</i> (RFID)	Bedasarkan penelitian yang dilakukan pada system kependudukan berbasis RFID. System ini dapat pengamanan data sidik jari pada <i>tag</i> RFID adalah data sidik jari yang di enkripsi (<i>chipertexs</i>).

3	Ahmaddul Hadi (2013)	Rancang Bangun Sistem Pengamanan Dokumen Pada Sistem Informasi Akademik Dengan Menggunakan Digital Signature	Pengamanan dokumen elektronik system informasi akademik (SIA) menggunakan digital signature dengan algoritma kurva eliptik dapat diimplementasikan dengan baik dan dibantu dengan barcode reader yang berfungsi membantu untuk menginputkan karakter ke form input, dan kecendrungan akan salah jika menggunakan keyboard yang diketikkan dengan tangan.
---	----------------------	--	--

I.6. Sistematika Penulisan

Untuk mempermudah dalam memperoleh gambaran mengenai permasalahan yang dibahas, maka dalam penulisan skripsi nantinya dibagi ke masing-masing bab tersebut adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini secara ringkas diterangkan mengenai latar belakang, identifikasi masalah, batasan masalah, tujuan penelitian dan manfaat penelitian, metodologi penelitian, serta sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Sub bab ini tentang teori yang berkaitan dengan pembuatan, desain dan tampilan rancangan aplikasi Implementasi pengamanan Data Teks Dalam Proses Transfer File dengan perangkat *android* pada Perangkat Android Dengan Algoritma RC4, serta teori-teori yang mendukung perancangan penelitian.

BAB III : ANALISIS DAN PERANCANGAN

Berisi tentang analisa dan perancangan aplikasi, yang meliputi analisa masalah, perancangan *interface*, perangkat yang digunakan, algoritma serta ketentuan penggunaan.

BAB IV : HASIL DAN UJI COBA

Berisi tentang tampilan hasil impelentasi program, beserta pembahasannya, serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini diuraikan kesimpulan dan saran yang dapat diberikan untuk pengembangan aplikasi yang dirancang.