BAB I

PENDAHULUAN

I.1. Latar Belakang

Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah Kriptografi, sedangkan langkah-langkah dalam kriptografi disebut algoritma kriptografi. Kriptografi merupakan suatu seni dimana sebuah data diamankan melalui proses penyandian. Pada permulaannya kriptografi digunakan untuk mengamankan sebuah data berupa teks. Bermacam-macam algoritma yang digunakan dalam mengamankan sebuah data.

Data dokumen merupakan data yang dapat digolongkan sebagai data pribadi. Salah satu cara mengamankan data dokumen itu memberikan pengamanan *file* tersebut. *File* dokumen yang berjenis teks di aplikasikan dengan perangkat lunak *notepad* atau *wordpad*. Data sebenarnya sifatnya rahasia karena seseorang yang menggunakan aplikasi wordpad isi dari surat menyurat ini sifatnya sangat rahasia sekali jika tidak dilakukan pengamanan maka isi surat tersebut bisa dirusak orang bukan itu saja tetapi isi dari surat itu dapat dibaca seseorang dan itu bisa disalahgunakan bagi orang yang tidak bertanggung jawab.

Dalam proses penyandian, penyandian yang digunakan adalah AES 192 *bit* merupakan proses penyandian kunci asimetris, sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima, dan disarankan bilangan prima yang besar. Hal ini digunakan untuk pencegahan usaha pemecahan *chipper text*, karena

semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya.

Berdasarkan uraian di atas penulis mengangkat judul ”**Mengamankan Record Database Algoritma AES 192 Berbasis Android**”

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan latar belakang masalah tersebut, maka Penulis dapat mengambil pokok permasalahan adalah sebagai berikut :

1. Untuk menghindari kerusakan dan keamanan data dari seseorang maka perlu dibuat sebuah aplikasi dalam penanganan data tersebut.
2. Agar aplikasi keamanan data tidak mudah ditembus maka perlu dibuat algoritma dalam penanganannya yaitu algoritma AES 192 *bit*.

I.2.2. Perumusan Masalah

Untuk membantu mengoptimalkan perancangan aplikasi enkripsi, maka perumusan masalahnya adalah sebagai berikut.

1. Bagaimana merancang aplikasi enkripsi atau pengamanan data di dalam sistem operasi *android*?
2. Bagaimana membangun aplikasi pengamanan data mudah digunakan?

I.2.3. Batasan Masalah

Mengingat luasnya ruang lingkup permasalahan yang dihadapi dalam penanganan program aplikasi pengamanan data dalam *android*, maka penulis membatasi ruang lingkup permasalahan pada :

1. Membuat aplikasi enkripsi berupa *field* didalam *database*.
2. Data yang dapat dienkripsi hanya berupa *field* tertentu.
3. Bahasa program yang digunakan adalah yang berjalan di android.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penyusunan skripsi ini adalah sebagai berikut :

1. Perancangan aplikasi *enkripsi* menggunakan sistem *mobile*.
2. Membangun aplikasi enkripsi yang sesuai guna membantu dalam penanganan keamanan data.
3. Untuk menambah minat dalam mempelajari tentang keamanan data menggunakan algoritma AES 192 *bit*.
4. Sebagai sarana untuk meningkatkan pengetahuan mengenai *android* dan sistem pemrogramannya.

I.3.2. Manfaat

Adapun manfaat yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

1. Untuk mengetahui peran android, khususnya meningkatkan perkembangan keamanan data.
2. Memberikan pengetahuan tentang algoritma AES yang dapat digunakan sewaktu-waktu bila dibutuhkan.
3. Sebagai bahan referensi bagi peneliti lain yang ingin merancang pengembangan aplikasi tentang AES 192 *bit*.

I.4. Metodologi Penelitian

Berisi langkah-langkah diperlukan untuk mencapai tujuan perancangan yang dilakukan. Adapun metodologi dalam pengumpulan data adalah:

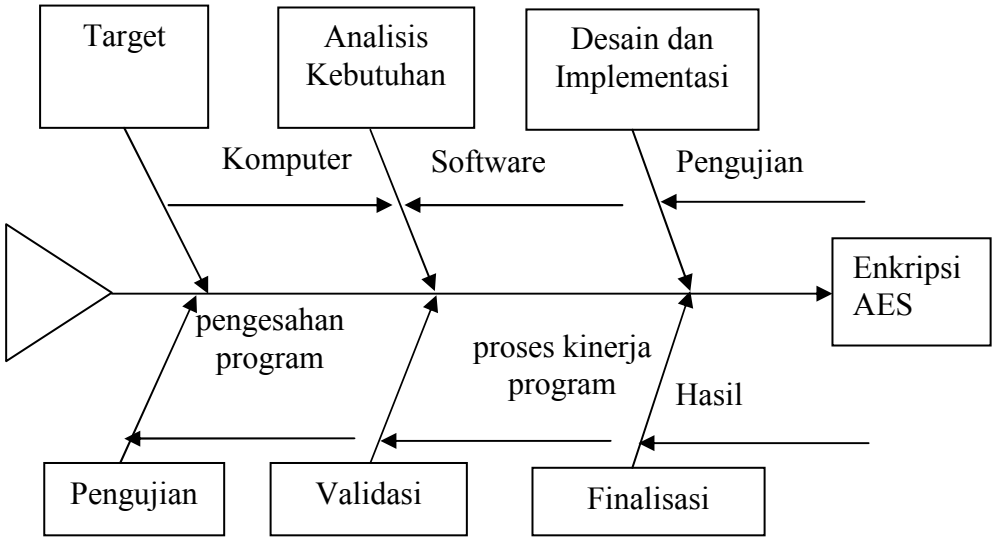
Studi Pustaka dan Literatur

Pada tahap ini dilakukan pengumpulan informasi yang diperlukan dalam berhitung. Informasi diperoleh dari literatur, buku-buku dan internet.

Implementasi

Implementasi yang dilakukan meliputi bangun ruang. Selain itu perancangan pengujian terhadap hasil juga dilakukan untuk mengetahui suatu algoritma.

Setelah melakukan penelitian lapangan dan penelitian kepustakaan penulis melanjutkan penelitian dengan prosedur sebagai berikut :



Gambar I.1. Prosedur Perancangan

a. Target

Membuat sistem keamanan data dengan AES 192 *bit* dengan maksud agar data lebih aman dari kerusakan.

b. Analisa kebutuhan

Untuk mencapai penyelesaian masalah, kebutuhan pokok yang harus ada pada sistem yang akan di bangun adalah :

1. Sistem keamanan data dengan AES 192 bit yang akan dibangun harus dapat di mengerti dengan mudah digunakan oleh pengguna.
2. Sistem dapat menampilkan hasil yang sebenarnya dari proses pengamanan data, dan mengeluarkan *output* berupa enkripsi dan deskripsi data.

c. Spesifikasi

Secara umum sistem keamanan data memiliki spesifikasi sebagai berukut :

a. Dalam Implementasi rancang program dibangun dengan menggunakan pemrograman *android* di dalam aplikasi *eclipse*.
b. Analisa yang mendeskripsikan perangkat yang dibutuhkan dalam pembangunan sistem yang terdiri dari perangkat keras dengan perangkt lunak komponen perangkat keras yang dibutuhkan oleh sistem adalah laptop.

d. Implementasi dan Verifikasi

Mengatur posisi yang tepat untuk form-form pada sistem, kemudian membentuk suatu logika yang diimplementasikan dengan bahasa pemrograman. Untuk mengetahui apakah sistem yang dirancang sudah dapat bekerja dengan baik maka perlu dilakukan verifikasi. Dengan demikian bila ada kesalahan atau kekurangan dapat diperbaiki terlebih dahulu.

e. Validasi

Setelah melewati tahap implementasi dan verifikasi maka tahap selanjutnya adalah validasi. Pada tahap ini dilakukan pengujian sistem secara menyeluruh, meliputi pengujian fungsional dan ketahanan sistem. Dari validasi ini dapat di ketahui kesesuain hasil perancangan dengan analisis kebutuhan yang diharapkan.

d. Finalisasi

Sistem sudah dapat digunakan dan dipublikasikan.

I.5. Kontribusi Penelitian

Keamanan data yang dilakukan karena ketidaknyamanan terhadap kerusakan dan penyalahgunaan terhadap data tersebut. Penelitian ini dirancang untuk memudahkan proses dalam hal keamanan data. Maka dari itu aplikasi ini diharapkan memberikan kontribusi yang besar. Kontribusi yang ingin dicapai yaitu :

1. Memanfaatkan teknologi sebagai alat keamanan data yang bermutu.
2. Memudahkan masyarakat dalam hal privasi terhadap data didalam dunia kerja
3. Menjadikan aplikasi untuk menyelamatkan data yang lebih baik.
4. Membangun teknologi informasi lebih bermutu dengan kriptografi.

I.6. Sistematika Penulisan

Adapun sistematika penulisan aplikasi enkripsi data pada skripsi ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini penulis akan menjelaskan mengenai latar belakang masalah dan ruang lingkup permasalahan yang terdiri dari : identifikasi masalah, perumusan masalah serta batasan masalah, tujuan dan manfaat, metodologi dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini berisi uraian mengenai teori-teori yang terkait dengan masalah yang diteliti, yaitu : pengertian sistem, penguasaan aplikasi dan UML.

BAB III : ANALISA DAN PERANCANGAN SISTEM

Pada bab ini penulis menjelaskan tentang analisis sistem yang terdiri dari : *input*, proses dan *output* serta evaluasi sistem yang berjalan dan desain sistem yang dibangun.

BAB IV : HASIL DAN UJI COBA

Pada bab ini penulis membahas tentang tampilan *interface* dan hasil serta pembahasan tentang enkripsi data yang dirancang serta kelebihan dan kekurangannya daripada sistem tersebut.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini penulis menguraikan kesimpulan dari keseluruhan penulisan dan saran yang membantu dalam penulisan.