BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan Teknologi Informasi dan Komunikasi pada saat ini sangatlah pesat. Tidak dapat dipungkiri bahwa kemajuan dan perkembangan teknologi mempunyai peranan penting dalam kehidupan manusia. Kemajuan teknologi dengan kehidupan manusia seakan-akan tidak dapat dipisahkan. Hal tersebut tentunya menyebabkan perubahan yang begitu besar terhadap kehidupan manusia di berbagai bidang serta memberikan dampak yang begitu besar, termasuk gaya hidup dan pola pikir masyarakat. Salah satu kemajuan teknologi informasi dan komunikasi yang paling signifikan pada saat ini adalah kemajuan teknologi mobile, seperti : Handphone, Smartphone, Tablet PC dan lain-lain. Dunia teknologi khususnya teknologi mobile memang sangat pesat perkembangannya, terlebih dengan adanya pertarungan berbagai merek dan Operating System yang semakin seru.

Perkembangan teknologi yang begitu pesat saat ini juga memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi dan data secara jarak jauh. Antar kota, wilayah, negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran informasi dan data. Seiring dengan itu tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitor oleh negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Kriptografi merupakan metode untuk mengamankan data, baik itu data teks maupun data gambar. Metode ini dilakukan dengan penyandian atau pengacakan data asli, sehingga pihak lain yang tidak mempunyai hak akses atas data tersebut tidak dapat memperoleh informasi yang ada di dalamnya. Hal ini dilakukan dengan alasan keamanan pada data yang dirahasiakan dan menghindari terjadinya kejahatan terhadap komputer. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Metode enkripsi yang dibahas adalah AES (Advanced Encryption Standard). AES (Advanced Encryption Standard) atau disebut Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu. Dalam kenyataannya sebuah algoritma kriptografi yang sudah ada sulit untuk dipelajari oleh seorang pemula. Oleh sebab itu algoritma tersebut sangat baik untuk keamanan data dalam berbagai aplikasi kriptografi.

Berdasarkan uraian di atas, penulis tertarik untuk mengajukan skripsi yang berjudul : **“Perancangan Aplikasi Enkripsi Teks menggunakan Metode AES berbasis Android”.**

I.2. Ruang Lingkup Permasalahan

Berdasarkan latar belakang di atas, penulis melakukan identifikasikan terhadap masalah yang akan diangkat dalam skripsi, merumuskannya serta membatasi permasalahan tersebut agar tidak menjadi terlalu luas.

I.2.1. Identifikasi Masalah

Berdasarkan uraian pada latar belakang masalah di atas, penulis melakukan identifikasikan beberapa permasalahan sebagai berikut.

1. Belum banyaknya aplikasi enkripsi teks yang tersedia untuk proses keamanan data teks dengan menggunakan metode AES (Advanced Encryption Standard).
2. Perlunya sebuah aplikasi berbasis android yang mempermudah proses enkripsi pada data teks untuk menjaga integritas dan keamanan pesan.
3. Masih minimnya aplikasi enkripsi data teks berbasis android yang menampilkan fitur yang menarik pada interface yang ditampilkan.

I.2.2. Rumusan Masalah

Berdasarkan uraian latar belakang terhadap masalah di atas, maka yang menjadi perumusan masalah adalah :

1. Bagaimana penerapan metode AES (Advanced Encryption Standard) pada aplikasi enkripsi teks yang dapat menjaga keamanan dan integritas data teks ?
2. Bagaimana merancang tampilan aplikasi berbasis android yang mempermudah proses enkripsi pada data teks untuk menjaga integritas dan keamanan pesan ?
3. Bagaimana membuat aplikasi enkripsi data teks berbasis android yang menampilkan fitur yang menarik pada interface yang ditampilkan.

I.2.3. Batasan Masalah

Untuk memberikan arahan yang jelas terhadap penulisan skripsi ini maka penulis memberi batasan terhadap permasalahan yang terjadi, yaitu :

1. Proses keamanan data teks menggunakan metode AES (Advanced Encryption Standard).

2. Pesan yang diproses enkripsi dan dekripsi adalah berupa teks.
3. Metode AES (Advanced Encryption Standard) hanya menggunakan ukuran blok dan kunci yang tetap sebesar 128.
4. Bahasa program yang digunakan adalah Java Eclipse.

I.3. Tujuan Dan Manfaat

Dari ruang lingkup permasalahan di atas, penulis menetapkan tujuan dan manfaat dari perancangan perangkat lunak yang diangkat dalam skripsi ini.

I.3.1 Tujuan

Adapun yang menjadi tujuan penulisan dalam penyusunan Skripsi adalah sebagai berikut :

1. Merancang dan membuat sebuah aplikasi untuk keamanan data teks.
2. Melakukan proses kriptografi terhadap data teks menggunakan metode AES (Advanced Encryption Standard).
3. Untuk menjaga integritas dan keamanan pesan dari pihak yang tidak berwenang.

I.3.2. Manfaat

Adapun manfaat yang akan di kemukakan dari penanganan masalah yang ada, yaitu:

1. Menjadikan suatu aplikasi keamanan data teks dengan menggunakan metode AES (Advanced Encryption Standard).
2. Menjadikan salah satu aplikasi yang bisa menjaga keamanan data teks agar tidak terjadi penyalahgunaan oleh pihak yang tidak bertanggung jawab dan juga menjamin keutuhan pesan.

I.4. Metodologi Penelitian

Pada pelaksanaan skripsi ini, adapun metode penelitiannya adalah sebagai berikut:

1. Observasi

   Pada tahap ini dilakukan eksplorasi terhadap beberapa perangkat dan konsep yang akan digunakan dalam membuat tugas skripsi. Eksplorasi dilakukan pada beberapa perangkat yang akan digunakan untuk membangun sistem dalam skripsi ini seperti *Eclipse*. Eksplorasi konsep dilakukan dengan cara studi literatur yaitu dengan studi dari berbagai macam buku teks, jurnal dan skripsi.

2. Analisis Algoritma

   Pada tahap ini dilakukan analisis terhadap kompleksitas algoritma AES (*Advanced Encryption Standard*) yang meliputi:

   a. kompleksitas algoritma pembangkitan kunci,

   b. kompleksitas algoritma enkripsi, dan

   c. kompleksitas algoritma dekripsi.

3. Analisis Keamanan

   Pada tahap ini dilakukan analisis keamanan algoritma AES (*Advanced Encryption Standard*) melalui telaah pustaka dari berbagai literatur. Literatur diambil dari buku, makalah, dan internet.

4. Analisis Hasil Implementasi

   Pada tahap ini dilakukan analisis uji running time terhadap hasil implementasi enkripsi dan dekripsi algoritma AES (*Advanced Encryption Standard*). Hal-hal yang diamati adalah, hasil dari enkripsi dan dekripsi teks yang dikombiasikan dengan kunci.

Adapun dua pendekatan yang dilakukan penulisan dalam melakukan pengujian sistem yang dibuat, yaitu :

a. Black Box Testing

Pengujian ini bertujuan untuk menunjukkan fungsi perangkat lunak tentang cara beroperasinya, apakah pemasukan data keluaran telah berjalan sebagaimana yang diharapkan dan apakah informasi yang disimpan secara eksternal selalu dijaga kemutakhirannya.

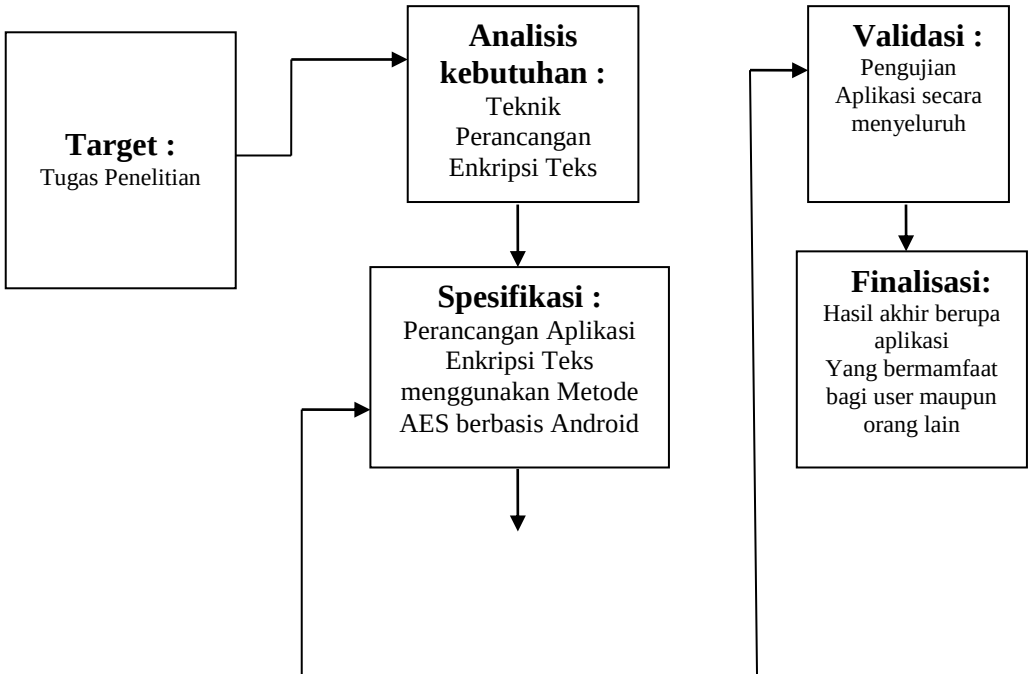
b. White Box Testing

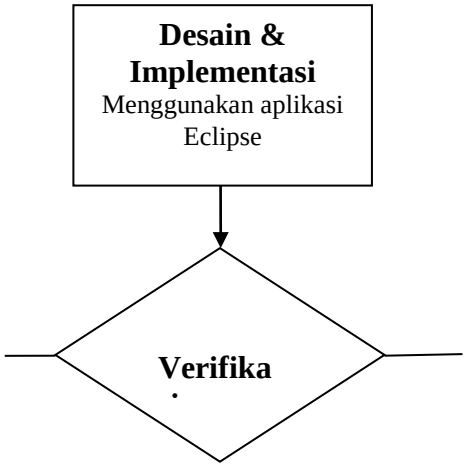
Pengujian ini dilakukan dengan meramalkan cara kerja perangkat lunak secara rinci, karenanya logical path (jalur logika) perangkat lunak akan ditest dengan menyediakan kasus pengujian yang akan mengerjakan kumpulan kondisi atau pengulangan secara spesisifik.

Selain itu terdapat beberapa prosedur pembuatan sistem sebagai berikut:

1. Prosedur Perancangan

Penelitian yang dilakukan berkaitan dengan desain dan implementasi aplikasi adalah sebagai berikut :





Gambar I.1 Prosedur Perancangan

2. Anasisis Kebutuhan

Analisis kebutuhan perangkat lunak (*software requirements analysis*) merupakan aktivitas awal dari siklus hidup pengembangan perangkat lunak. Tahap analisis adalah tahapan pengumpulan kebutuhan-kebutuhan dari semua elemen sistem perangkat lunak yang akan dibuat.

Adapun analisis kebutuhan dalam rancangan sistem yang akan dibangun adalah sebagai berukut :

a. Data atau informasi apa yang akan diproses merupakan data langkah pembuatan aplikasi.

b. Fungsi apa yang diinginkan yaitu program yang dirancang merupakan aplikasi Eclipse.

1. Spesifikasi dan Desain

Spesifikasi kebutuhan perangkat lunak atau *Software Requirements Spefication* (SRS) adalah sebuah dokumen yang berisi pernyataan lengkap dari apa yang dapat dilakukan oleh perangkat lunak, tanpa menjelaskan bagaimana hal tersebut dikerjakan oleh perangkat lunak. Suatu SRS harus mencantumkan tentang deskripsi dengan lingkungannya.

Adapun spesifikasi kebutuhan di dalam membangun perangkat lunak yang akan di rancang adalah sebagai berikut :

a. Spesifikasi Perangkat Keras

Spesifikasi perangkat keras yang dibutuhkan yaitu :

i. *Processor Intel Core i3* 2,2 Ghz

ii. *Ram 2 GB*

iii. *Hardisk 500 GB*

iv. *Intel HD 3000*

v. *32-bit Operating system*

vi. *Mouse*

b. Spesifikasi Perangkat Lunak

Adapun spesifikasi perangkat lunak yang dibutuhkan yaitu:

i. Sistem Operasi Windows 7

ii. Eclipse

2. Implementasi dan Verifikasi

Perancangan adalah langkah awal pada tahap pengembangan suatu sistem. Perancangan dapat didefinisikan sebagai proses untuk mengaplikasikan berbagai macam teknik dan prinsip untuk tujuan pendefinisian secara rinci suatu perangkat, proses atau sistem agar dapat direalisasikan dalam suatu bentuk fisik.

Sedangkan Implementasi merupakan tahap pengkodean yang merupakan suatu proses translasi. Rancangan detil ditranslasikan ke dalam suatu bahasa pemrograman. Bahasa pemrograman adalah alat yang digunakan untuk komunikasi antara manusia dan komputer. Verifikasi program merupakan suatu metode yang digunakan untuk menjamin kebenaran suatu program. Metode ini mencegah terjadinya kesalahan dengan memberikan jaminan kebenaran berdasarkan komputasi matematis. Tentunya metode ini berbeda dengan testing yang menjamin program dengan

mencari kebenaran dan kesalahan lewat sejumlah data sebagai masukan. Verifikasi program melakukan simbolisasi masukan sehingga jaminan diberikan untuk semua data yang berlaku sebagai masukan.

3. Validasi

Validasi merupakan proses untuk menunjukkan seberapa besar nilai keakuratan program terhadap kondisi-kondisi saat pemakaian sebenarnya. Proses ini menjalankan skenario berdasarkan data dan lingkungan yang merepresentasikan dunia nyata dengan menggunakan mesin percobaan.

4. Finalisasi

Finalisasi merupakan istilah generik yang merujuk pada tahapan akhir prosedur didalam perancangan perangkat lunak yaitu dengan menginstall atau memasang perangkat lunak yang telah selesai kedalam komputer pengguna.

I.4.1. Analisa Tentang Sistem Yang Ada.

Metode yang penulis gunakan dalam penulisan skripsi ini mulai dari pengumpulan data hingga nanti sampai kepada terselesaikannya skripsi ini adalah sebagai berikut :

1. Studi Kepustakan (*Library Research*)

   Memperoleh data dengan membaca buku-buku, serta majalah yang berhubungan dengan masalah yang sedang dibahas.

2. Internet (*Surfing*)

   Memperoleh data dari situs-situs yang berhubungan dengan masalah yang sedang dibahas dan men-*download*-nya sebagai bahan referensi. Dalam hal ini penulis melakukan *download* terhadap dokumentasi-dokumentasi, FAQ (*Frequently Asked Questions*), RFC (*Request For*

Comments) dan *How to Manual* yang terdapat pada situs-situs yang berhubungan dengan masalah yang sedang dibahas.

I.4.2. Pengujian / Uji Coba Sistem

Dalam pengujian ini penulis menguji coba Aplikasi enkripsi teks menggunakan metode AES ini dengan menggunakan Eclipse sebagai *Software*, aplikasi ini akan berfungsi jika Aplikasi enkripsi teks menggunakan metode AES ini tidak mengalami kesalahan *coding script*, dan hasilnya akan menampilkan Aplikasi enkripsi teks menggunakan metode AES berbasis Android.

I.5. Sistematika Penulisan

Sistematika penulisan ini terdiri dari V bab, dengan tujuan untuk mempermudah dalam pembahasan. Adapun sistematika penulisan tersebut adalah sebagai berikut :

BAB I : PENDAHULUAN

Pendahuluan 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 tentang teori dasar yang berhubungan dengan program yang dirancang, serta bahasa pemrograman yang digunakan.

BAB III : ANALISIS MASALAH DAN RANCANGAN PROGRAM

Pada bab ini mengemukakan tentang analisis masalah program yang akan dirancang dan rancangan program yang digunakan dalam penulisan skripsi ini.

BAB IV : IMPLEMENTASI DAN ANALISIS PROGRAM

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

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penelitian dan saran dari penelitian sebagai perbaikan di masa yang akan datang.