BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kriptografi merupakan suatu seni dalam pengamanan data. Pada mulanya kriptografi digunakan untuk mengamankan sebuah data berupa teks. Proses yang dilakukan oleh kriptografi yaitu enkripsi dan deskripsi, di mana pesan (*plaintext*) dienkripsi dan menghasilkan *ciphertext*, lalu *ciphertext* di deskripsi menjadi *plaintext* lagi. Bermacam-macam algoritma yang digunakan dalam mengamankan sebuah data diantaranya yaitu DES, RC6, RSA, AES, dan masih banyak lagi algoritma kriptografi lainnya. Kriptografi sudah ada sejak jaman dahulu kala, contohnya yang dilakukan oleh Tentara Sparta (Yunani) 400 SM mereka membuat pesan untuk menyerang, dan dikirimkan ke tentara Yunani yang lain, agar menyerang secara bersamaan.

Algoritma kriptografi yang sudah ada pada masa lampau juga beraneka macam. Salah satu algoritma Kriptografi pada masa lampau seperti algoritma caesar cipher, subtitusi dan juga tranposisi, tentu algoritma kriptografi masih sangat banyak, dari masa lampau hingga sekarang. Untuk dapat membuat sebuah aplikasi yang menggunakan sistem keamanan kita harus mengetahui algoritma-algoritma yang sesuai dengan aplikasi yang kita buat, dengan mengetahui algoritma-algoritma kriptografi yang sangat banyak akan membuat kita menjadi tertarik untuk mempelajari kriptografi

lebih dalam. Pengalaman pribadi peneliti pada skripsi ini yaitu peneliti mengalami kesulitan untuk mencari algoritma tertentu, dikarenakan banyaknya sumber yang memberikan info berbeda .Oleh karena itu peneliti pada skripsi ini akan merangkum dan mengumpulkan algoritma-algoritma kriptografi dalam sebuah aplikasi android yang bernama "kriptopedia". Aplikasi ini dibuat dengan sistem operasi android karena perkembangan *smartphone* yang sedang populer saat ini adalah *smartphone* yang berbasis android, dan juga sangat praktis untuk dibawa kemana pun dan dapat dipelajari kapan pun.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang masalah di atas maka permasalahan utama adalah "bagaimana merancang aplikasi ensiklopedia kriptografi serta demo algoritma kriptografi berbasis android?".

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas maka didapat batasan-batasan masalah yang digunakan untuk membatasi ruang lingkup masalah dalam melakukan penelitian. Batasan masalah yang digunakan adalah sebagai berikut:

1. Perangkat yang mendukung sistem operasi android dengan minimal versi yang dibutuhkan adalah versi 2.2 (froyo).
2. Aplikasi digunakan sebagai media pembelajaran mengenai algoritma-algoritma kriptografi.

3. *Software* yang digunakan dalam perancangan adalah Android Developer Tools (ADT).
4. Demo aplikasi yang dibuat hanya algoritma modern saja.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian adalah untuk membuat aplikasi kriptopedia berbasis android sesuai dengan yang telah dijabarkan dalam batasan masalah.

1.5 Manfaat Penelitian

Dengan melakukan penelitian yang menghasilkan aplikasi maka diharapkan didapatkan manfaat-manfaat sebagai berikut:

1. Bagi penulis:

   Menerapkan salah satu disiplin ilmu sesuai dengan kompetensi yang didapatkan selama masa perkuliahan dan dapat membantu mengenalkan berbagai macam algoritma-algoritma kriptografi yang ada hingga sekarang.

2. Bagi Pengguna:

   Dapat digunakan sebagai media pembelajaran mengenai algoritma-algoritma kriptografi dengan praktis karena sifatnya aplikasi *mobile*, sehingga diharapkan dapat meningkatkan ketertarikan masyarakat mengenai kriptografi.

1.6 Metode Penelitian

Langkah-langkah dalam melakukan penelitian yang berjudul "Aplikasi Kriptopedia Berbasis Android" adalah sebagai berikut:

1. Pengumpulan Data

   Pengumpulan data yang dilakukan oleh penulis salah satunya adalah dengan mencari referensi dari buku yang memuat informasi mengenai algoritma-algoritma kriptografi.

2. Analisa Data

   Melakukan analisa pada data-data yang telah diperoleh agar data yang akan digunakan dapat benar-benar menunjang aplikasi yang akan dibuat sehingga dapat mencapai tujuan yang diinginkan.

3. Perancangan Aplikasi

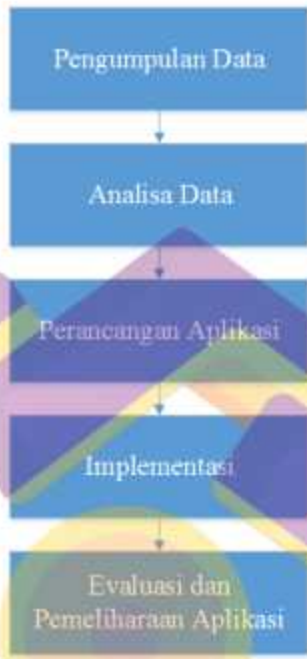
   Melakukan perancangan awal untuk membangun aplikasi agar nantinya dalam proses pembuatan menjadi lebih terstruktur dan dapat mencapai tujuan yang diinginkan.

4. Implementasi

   Rancangan dalam proses perancangan dituangkan dalam bahasa pemrograman sehingga menghasilkan aplikasi yang akan diimplementasikan untuk mengatasi masalah yang telah disebutkan.

5. Evaluasi dan Pemeliharaan Aplikasi

   Melakukan evaluasi pada aplikasi yang telah dibangun dan diimplementasikan berdasarkan masalah dan tujuan yang akan dicapai serta melakukan pemeliharaan seperti memperbaiki informasi dan panduan di dalam aplikasi maupun menambahkan fitur lain jika dinilai diperlukan untuk mencapai tujuan yang diinginkan.



Gambar 1.1 Metode Penelitian

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Bab pendahuluan ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan yang digunakan dalam penulisan skripsi

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, berisi dasar-dasar teori yang digunakan dalam penyusunan skripsi serta perancangan dan pembuatan

aplikasi. Pada bab ini juga berisi tentang perangkat lunak yang digunakan dalam pembuatan aplikasi.

BAB III ANALISIS DAN PERANCANGAN

Pada bab analisis dan perancangan menguraikan tentang gambaran umum aplikasi, analisis terhadap kasus yang diteliti, dan perancangan aplikasi yang dibuat.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini memaparkan hasil tahapan penelitian mulai dari analisis, desain, implementasi desain, hasil testing dan implementasinya.

BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian serta saran guna memperbaiki kelemahan dan kekurangan yang ada pada aplikasi.