

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi *mobile* berkembang sangat pesat seiring dengan munculnya sistem operasi android, dimana android dapat dikembangkan secara terbuka (open source), sehingga memicu munculnya berbagai aplikasi yang membantu aktifitas manusia, salah satunya untuk keperluan aspek keamanan. Android telah menyediakan API (Application Programming Interface) khusus untuk fungsi-fungsi kriptografi, seperti enkripsi, dekripsi.

Kriptografi adalah salah satu cabang ilmu yang menyediakan teknik-teknik yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data, dan sebagainya. Banyak perusahaan maupun pemerintahan mengimplementasikan kriptografi dalam pengamanannya seperti ATM, E-KTP, GSM dan lain-lain. Implementasi kriptografi pada aplikasi *mobile* mempunyai beberapa manfaat, seperti meningkatkan efektifitas karena fleksibilitas dalam hal tempat, meningkatkan keterlibatan pengguna, menonjol dalam persaingan, memberikan kemudahan pengguna (User Experience) lebih baik, performa yang cepat.

Mengelola kalender merupakan salah satu bagian terpenting dari agenda. Perkembangan teknologi mempengaruhi pengelolaan kalender setiap manusia. Kalender yang dulunya digunakan sebagai penanda suatu agenda dan ada di setiap rumah, kini ada di setiap *smartphone*. Fiturnyapun semakin berkembang, seperti

adanya reminder dan note. Namun dari semua aplikasi yang ditawarkan tidak banyak yang memberikan layanan keamanan. Padahal banyak orang menuliskan catatan, perencanaan maupun agenda bersifat pribadi yang seharusnya tidak boleh diketahui orang lain.

Fitur yang banyak muncul pada kalender tanpa adanya keseimbangan pada keamanan akan menimbulkan kerugian. Contohnya apabila seseorang membuat perencanaan yang bersifat rahasia, tanpa adanya pengaman, orang lain dapat dengan mudah membaca dan menggagalkan perencanaan yang sudah disusun. Dengan adanya algoritma kriptografi dapat mengamankan perencanaan tersebut, serta membuat algoritmanya berlapis di yakini akan membuat informasi tersebut memiliki level keamanan lebih tinggi.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut maka permasalahan yang dapat dirumuskan adalah Bagaimana merancang aplikasi kalender dengan menerapkan algoritma kriptografi caesar, vigenere dan blok cipher berbasis Android?

1.3 Batasan Masalah

Agar pembahasan tidak meluas maka penulis memberikan batasan masalah, adapun batasan masalahnya sebagai berikut:

1. Aplikasi ini merupakan implementasi algoritma kriptografi yang di terapkan pada kalender.
2. Aplikasi ini hanya menggunakan algoritma kriptografi meliputi : caesar, vigenere dan blok cipher saja dalam proses enkripsi dan dekripsi teks.

3. Aplikasi ini tidak menggunakan akses jaringan internet (Offline).
4. Aplikasi ini dijalankan pada *smartphone* yang menggunakan sistem operasi Android 4.0 Ice Cream Sandwich ke atas.
5. Perangkat lunak yang digunakan untuk membuat aplikasi adalah Android Studio dan Database SQLite.
6. Aplikasi ini hanya membahas masalah keamanan tulisan berdasarkan aspek keamanan kriptografi yaitu *confidentiality* dan *integrity*.

1.4 Maksud dan Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk membuat aplikasi Kalender berbasis android dengan kerahasiaan isi Kalender lebih baik karena perencanaan yang dibuat akan dienkripsi dengan algoritma kriptografi berlapis yaitu caesar, vigenere dan blok cipher.

1.5 Metode Penelitian

Untuk mempermudah dalam proses penelitian penulis membagi Metode Penelitian menjadi beberapa bagian dalam pengolahan data dan informasi yang digunakan untuk penyusunan skripsi ini antara lain :

1.5.1 Metode Pengumpulan Data

Metode-metode pengumpulan data yang digunakan dalam pembuatan sistem ini adalah sebagai berikut :

a. Studi Kepustakaan

Metode Pengumpulan data dilakukan dengan cara pembelajaran literatur. Pada tahap ini dilakukan studi kepustakaan melalui membaca referensi dari berbagai sumber dan buku yang diperoleh dari perpustakaan, koleksi pribadi.

b. Konsultasi

Melakukan diskusi dengan dosen pembimbing mengenai topik dan permasalahan yang terdapat dalam penelitian.

1.5.2 Metode Analisis Data

Semua data yang terkumpul dari studi pustaka akan dianalisis untuk mendapatkan hasil untuk pemecahan masalah yang timbul. Adapun metode yang digunakan untuk menganalisis yaitu metode SWOT dan metode Kebutuhan fungsional dan kebutuhan non fungsional.

1.5.3 Metode Perancangan

Metode perancangan yang digunakan dalam penulisan laporan penelitian ini adalah :

- a. Perancangan basis data dibuat dengan menggunakan diagram ERD (*Entity Relationship Diagram*).
- b. Perancangan aplikasi dibuat dengan model UML (*Unified Modeling Language*) menggunakan *use case*, *activity diagram*, *class diagram* dan *sequence diagram*.
- c. Membuat rancangan tampilan.

1.5.4 Pengembangan Sistem

Metode yang digunakan dalam pengembangan sistem ini adalah metode *Waterfall*. Model air terjun (*waterfall*) sering juga disebut model sekuensial linier (*sequential linear*) atau alur hidup klasik (*classic life cycle*) yang dimulai dari analisis, desain, pengkodean, pengujian, dan tahap pendukung (*support*).

1.5.5 Metode *Testing*

Metode pengujian sistem yang digunakan adalah *Black Box* dan *White Box*.

1.6 Sistematika Penulisan

Laporan penelitian ini akan disusun secara sistematis kedalam 5 bab, masing-masing bab akan diurutkan sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan membahas mengenai latar belakang masalah, perumusan masalah, batasan masalah, maksud dan tujuan penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan membahas mengenai penelitian terdahulu dan dasar-dasar teori yang dipergunakan dalam membuat sistem dan membahas secara singkat tentang bahasa pemrograman yang akan digunakan dalam skripsi ini.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan memaparkan tentang gambaran umum serta menguraikan tentang analisis terhadap permasalahan yang ada seperti kebutuhan apa saja yang diperlukan untuk membuat aplikasi, UML, rancangan *interface* dan rancangan tentang aplikasi yang akan dibuat.

BAB IV IMPLEMENTASI SISTEM

Bab ini memberikan penjelasan tentang pembuatan aplikasi mobile berbasis android dan cara pengoperasiannya.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil dari semua tahap yang telah dilalui selama penulisan serta saran-saran dalam pembuatan skripsi ini.

DAFTAR PUSTAKA

Berisi sumber-sumber bacaan yang digunakan sebagai bahan acuan dalam penelitian ini.

