BAB I
PENDAHULUAN

1.1 Latar Belakang

Telepon selular(ponsel) semakin berkembang dari hari ke hari, tidak hanya dari sudut teknologi tetapi juga dari sudut tampilan atau *look and feel*. Selain sebagai alat untuk berkomunikasi, ponsel juga menjadi alat untuk melakukan berbagai komunikasi yang lainnya seperti *e-mail*, *internet*, *fax* dan sebagainya. Ponsel dengan *feature* lengkap dan memiliki teknologi yang tinggi dapat dikatakan sebagai sebuah *smartphone*. Kehadiran *smartphone* termasuk yang berbasiskan *Android* membuat para programmer berlomba-lomba untuk membuat aplikasi yang dapat digunakan dan disukai oleh pengguna *smartphone*. Sehingga banyak sekali pilihan aplikasi-aplikasi yang dapat dinikmati.

Disadari atau tidak kebanyakan dari mereka memasangkan aplikasi catatan pada *smartphonenya* hal ini dikarenakan orang-orang sering menyimpan catatan untuk alasan sebagai pengingat, penyimpan jadwal, dan penyimpan tulisan-tulisan penting. Sehingga catatan *elektronik* yang menjadi privasi seseorang harus terjaga kerahasiannya. Untuk itu dibutuhkan teknik penyandian teks yang membuat teks menjadi sebuh karakter yang tidak dapat difahami bacaannya.

Berdasarkan hal tersebut maka diperkenalkanlah konsep pengamanan kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasian, integritas data, serta otentifikasi, **(5)**. Ada beberapa contoh macam-macam metoda

kriptografi untuk membuat pesan rahasia antara lain: *Caesar*, *Affine*, *Monoalphabetic*, *Polyalphabetic*, *Vigenere*, *Playfair*, Transposisi, MD5, DES, RSA, DSA, *ElGamal*, dan SHA. Bahkan sekarang telah digunakan kriptografi hibrida untuk menggabungkan dua metoda kriptografi. Kriptografi Hibrida adalah suatu algoritma yang memadukan kriptografi kunci simetris dengan kriptografi kunci public. Kriptografi hibrida ini memanfaatkan dua tingkatan kunci yaitu kunci simetris untuk enkripsi dan dekripsi pesan dan pasangan kunci privat dengan kunci publik untuk melindungi kunci simetris, **(1)**.

Dari pernyataan tersebut penyusun tertarik untuk membuat sebuah catatan *elektronik* pada *smartphone* berbasis *Android* yang dirahasiakan dengan metoda kriptografi hibrida dari metoda *Ron Shamir Adleman* (RSA) dan *Advanced Encryption Standard* (AES)-128. Hal ini berdasarkan pernyataan bahwa salah satu agoritma enkripsi modern yang menjadi standar saat ini adalah algoritma AES(*Advanced Encryption Standard*), algoritma AES merupakan salah satu algoritma enkripsi kunci simetris, yaitu algoritma yang menggunakan kunci enkripsi yang sama dengan kunci yang digunakan untuk dekripsi, sehingga hanya pihak yang memiliki kuncinya saja yang dapat membaca isi data yang telah dienkripsi tersebut. Sejak November 2001 AES telah digunakan oleh NIST(*National Institute of Standards an Technology*) sebagai standar pemrosesan data untuk informasi federal, kemudian dilanjutkan pada bulan Juni 2003 pemerintah Amerika mengumumkan bahwa AES cukup aman untuk memproteksi informasi, **(2)**. Dan Algoritma RSA sebagai salah satu algoritma kriptografi kunci publik(asimetris), yaitu kunci yang digunakan untuk enkripsi berbeda dengan

kunci yang digunakan untuk dekripsi, sehingga memungkinkan kedua belah pihak yang saling bertukar pesan memiliki kunci enkripsi dan dekripsi masing masing. Algoritma ini ditemukan oleh tiga orang peneliti dari MIT(*Massachussets Institute of Technology*) pada tahun 1976, mereka adalah Ron Rivest, Adi Shamir, dan Leonard Adleman, **(2)**.

Kedua Algoritma memiliki kelebihan dan kekurangan masing-masing maka jika keduanya digabungkan dengan metoda hibrida maka kelebihan dari RSA akan mengurangi kekurangan dari AES, begitu juga kelebihan dari AES akan mengurangi kekurangan dari RSA. Sehingga diharapkan akan menciptakan metoda kriptografi hibrida untuk penyandian teks yang lebih sulit untuk dipecahkan.

Berdasarkan dasar pemikiran tersebut, maka dalam penyusunan laporan tugas akhir ini akan mengangkat judul "**Aplikasi Kriptografi Hibrida untuk Catatan Berbasis Android**". Dengan dibuatnya laporan tugas akhir ini diharapkan dapat menjelaskan karakteristik aplikasi yang akan penyusun jadikan sebagai tugas akhir dan akan menjadi solusi dari permasalahan diatas.

1.2 Rumusan Masalah

Berdasarkan dari uraian latar belakang di atas maka dapat dirumuskan suatu permasalahan yaitu, bagaimana memodelkan rancangan suatu aplikasi kriptografi hibrida dan mengimplementasikannya pada *smartphone* berbasis Android?

1.3 Tujuan

Berdasarkan permasalahan yang diteliti, maka tujuan dari penyusunan tugas akhir ini adalah sebagai berikut:

1. Membuat suatu aplikasi kriptografi untuk pengamanan catatan pada *platform* Android dengan menerapkan metoda kriptografi hibrida.
2. Mengimplementasikan metoda kriptografi pada sebuah aplikasi dengan menggunakan bahasa pemrograman java.
3. Mengamankan kerahasian catatan penting seperti no-rekening, password, atau catatan-catatan yang mengandung unsur *privasi* lainnya dan tersimpan pada *smartphone* berbasis Android.

1.4 Batasan Masalah

Agar dalam pengerjaan tugas akhir ini dapat lebih terarah dan tidak terlalu meluas, maka penyusun menentukan batasan-batasan dalam pembuatan aplikasi kriptografi hibrida untuk catatan berbasis android ini, adapun batasan-batasan tersebut adalah sebagai berikut:

1. Aplikasi ini memilik fitur utama yaitu membuat, menyimpan, merubah, menghapus catatan *elektornik* dan mengubahnya kedalam bentuk enkripsi, kemudian untuk dapat membukanya digunakan dekripsi dengan *key* yang hanya diketahui pembuat *catatan.*
2. Aplikasi ini menerapkan metoda *kriptografi* hibrida dari Algoritma *Ron Shamir Adleman* (RSA) dan *Advanced Encryption Standard* (AES)-128.

3. Penulisan metoda *Rational Unified Process* (RUP) yang digunakan pada laporan tugas akhir ini merupakan keseluruhan persiapan *requirement*, *analysis, desaign, implementation* dan *testing.* Yang dicantumkan pada Bab I.
4. Fase *Transition* pada metoda *Rational Unified Process* (RUP) tidak digunakan pada laporan tugas akhir ini sehingga aplikasi belum diluncurkan ke komunitas pengguna.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan dalam penyusunan laporan tugas akhir ini terdiri dari dua bagian, yaitu teknik pengumpulan data dan metoda pengembangan perangkat lunak, **(11)**.

1. Teknik pengumpulan data

   Beberapa teknik yang digunakan dalam mengumpulkan data dalam laporan tugas akhir ini adalah:

   a. Studi *literature*

      Pengumpulan data dengan cara mengumpulkan bacaan-bacaan yang berkaitan dengan masalah yang diteliti, mempelajari buku-buku referensi, website, jurnal, papers dan bacaan-bacaan lain yang berhubungan dengan Android dan Kriptografi.

   b. *Interview*

      Teknik pengumpulan data dengan melakukan konsultasai kepada dosen pembimbing tugas akhir, dosen mata kuliah yang bersangkutan, maupun

dengan teman guna mendapatkan informasi yang berkaitan dengan pokok bahasan.

2. Metoda Pengembangan Perangkat Lunak

Metoda pengembangan perangkat lunak yang digunakan dalam penelitian ini adalah Rational Unified Process (RUP). *Rational Unified Process* (RUP) merupakan suatu metode rekayasa perangkat lunak yang dikembangkan dengan mengumpulkan berbagai *best practises* yang terdapat dalam industri pengembangan perangkat lunak. Ciri utama metode ini adalah menggunakan *use-case driven* dan pendekatan iteratif untuk siklus pengembangan perangkat lunak. RUP menggunakan konsep *object oriented*, dengan aktifitas yang berfokus pada pengembangan model dengan menggunakan *Unified Model Language* (UML), **(10)**.

Adapun *fase-fase* dari metoda *Rational Unified Process* (RUP) yang akan penyusun gunakan pada laporan tugas akhir ini adalah:

a. *Inception*

1. Pada *fase* ini pengembang menentukan ruang lingkup dan pemodelan sistem dengan *unified modelling language*. Tahapan-tahapan yang akan dilakukan adalah sebagai berikut:
2. Menentukan Ruang Lingkup
    a. Analisis Masalah.
    b. Analisis Pemecahan Masalah.
    c. Analisis Kriptografi Hibrida(RSA dan AES-128).

3. Pemodelan Sistem dengan Unified Modelling language

    a. Use Case Diagram.

    b. Class Diagram.

    c. Statechart Diagram.

    d. Activity Diagram.

    e. Sequence Diagram.

b. *Elaboration*

Pada tahap ini dilakukan perancangan perangkat lunak mulai dari menspesifikasikan fitur perangkat lunak, dan perancangan *interface*. Tahapan-tahapan yang akan dilakukan adalah sebagai berikut:

1. Menganalisa berbagai persyaratan

    a. Analisis Kebutuhan Fungsional.

        Pada tahap ini dilakukan penentuan *fiture-fiture* yang akan diterapkan pada aplikasi. Adapun *fiture-fiture* pada aplikasi yang akan dibuat adalah:

        a. Mampu membuat, menyimpan, merubah, dan menghapus sebuah catatan.

        b. Terdapat pilihan enkripsi dan dekripsi disertai kunci yang dapat ditentukan sendiri.

        c. Terdapat informasi mengenai aplikasi dan cara penggunaannya.

        d. Terdapat beberapa daftar istilah-istilah kriptografi.

        e. Terdapat informasi mengenai kriptografi.

b. Analisis Kebutuhan Non-Fungsional.

a. Kebutuhan Perangkat Lunak.

b. Kebutuhan Perangkat Keras.

c. Kebutuhan User.

2. Perancangan Sistem

a. Perancangan Database.

b. Perancangan Struktur Aplikasi.

c. Perancangan Antarmuka(*interface*).

3. *Construction*

Pada tahap ini dilakukan pengimplementasian analisis sistem, rancangan database, pemodelan sistem, rancangan *interface* dan menentukan hasil akhir dari fase Constuction. Tahapan-tahapan yang akan dilakukan adalah sebagai berikut:

1. Implementasi Sistem.

a. Persiapan Kebutuhan Sistem.

b. Cara Penggunaan.

c. Pengujian.

2. Implementasi Kriptografi Hibrida(RSA dan AES-128).

Mengimplementasikan hasil analisis pokok bahasan dari tugas akhir yaitu, kriptografi hibrida dari algoritma Ron Shamir Adleman(RSA) dan *Advanced Encryption Standard*(AES)-128 kedalam sebuah *class*.

3. Implementasi Rancangan Database.
4. Implementasi pemodelan dan interface Sistem.
5. Pengujian Sistem.
6. Hasil Akhir Fase Construction.

Hasil akhir dari fase ini adalah pengembangan versi alpha menjadi aplikasi yang siap untuk dirilis dan dipublikasikan. Selain itu aplikasi telah disertai dengan laporan atau dokumentasinya.

1.6 Sistematika Penulisan

Untuk menghasilkan laporan Tugas Akhir yang mudah dipahami, maka perlu adanya suatu sistematika penulisan yang terstruktur dengan baik. Berikut dijelaskan sistematika yang dipakai oleh penyusun dalam penyelesaian laporan Tugas Akhir ini:

BAB I PENDAHULUAN

Bab ini menguraikan latar belakang masalah, perumusan masalah yang merumuskan berbagai masalah yang diteliti secara lebih jelas, batasan masalah untuk memberikan batasan yang tegas dan jelas serta sistematika penulisanan yang menguraikan urutan penyajian yang digunakan dalam penyusunan tugas akhir ini.

BAB II LANDASAN TEORI

Bab ini membahas tentang landasan teori dari topik penyusunan tugas akhir secara mendalam beserta dengan referensinya.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menguraikan hasil analisis dan perancangan sistem yang akan dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini akan menguraikan implementasi sistem yang telah dianalisa dan dirancang sebelumnya kemudian melakukan pengujian terhadap sistem.

BAB V PENUTUP

Bab ini berisi uraian tentang kesimpulan, usulan, solusi dan saran terhadap aplikasi yang hendak dibangun dan bila akan dikembangkan lebih lanjut.