

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Di era kemajuan teknologi saat ini, mungkin penggunaan pesan singkat atau yang lebih dikenal dengan SMS (*Short Message Service*) sudah mulai jarang. Karena beberapa kalangan masyarakat sudah menggunakan ponsel pintar atau *smartphone* khususnya android untuk melakukan komunikasi atau pertukaran data melalui koneksi internet. Sehingga banyak sekali aplikasi-aplikasi *instant messenger* yang digunakan seperti whatsapp, line, BlackBerry Messenger (BBM), wechat dan lain-lain.

Namun tidak sedikit pengguna *smartphone* Android yang masih menggunakan SMS sebagai media komunikasi mereka karena berbagai alasan misalnya harga paket internet yang cukup mahal. Tetapi tingkat keamanan SMS sangatlah rendah, karena SMS tidak melalui proses enkripsi melainkan hanya diubah kedalam bentuk heksadesimal atau PDU (*Protocol Data Unit*) di server operator, sehingga pesan tersebut masih bisa dicuri atau disadap oleh pihak yang tidak bertanggungjawab.

Kriptografi dapat digunakan untuk mengamankan data, khususnya SMS. Mungkin ada beberapa aplikasi untuk mengamankan pesan berbasis android yang menggunakan ilmu kriptografi di dalamnya. Namun aplikasi-aplikasi tersebut hanya menggunakan satu metode kriptografi saja, entah itu menggunakan metode kriptografi simetri ataupun kriptografi asimetri.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, rumusan masalahnya adalah:

1. Bagaimana mengimplementasikan algoritma RSA, 3DES, dan MD5 menggunakan bahasa pemrograman JAVA pada IDE eclipse?
2. Bagaimana merancang suatu aplikasi SMS berbasis android dengan nama "Hybridcrypto Messenger" menggunakan metode *hybrid cryptosystem*?
3. Bagaimana cara menggunakan aplikasi "Hybridcrypto Messenger"?

1.3 Batasan Masalah

Agar pembahasan lebih terfokus, maka penulisan skripsi dibatasi pada beberapa hal, yaitu :

a) Ruang Lingkup Penelitian

1. Penelitian tentang teknologi android.
2. Aplikasi hanya dapat dijalankan pada telepon seluler yang mendukung sistem operasi Android minimal versi 2.3.
3. Penelitian tentang ilmu kriptografi khususnya *hybrid cryptosystem*.
4. Penelitian tentang algoritma RSA, 3DES dan MD5.
5. (e) pada *Public Key RSA default* = 131.
6. Panjang karakter SMS (*plaintext*) dibatasi maksimal 160 karakter.

b) Software yang digunakan :

1. Eclipse Kepler
2. Java Development Tools (JDK)
3. Android Software Development Kit (SDK)
4. Android Development Tools

1.4 Maksud dan Tujuan Penelitian

Beberapa tujuan yang ingin dicapai penulis dalam penelitian ini antara lain adalah :

1. Menerapkan ilmu teori dan praktikum yang didapat selama mengikuti pendidikan di STMIK AMIKOM Yogyakarta khususnya pada mata kuliah kriptografi dan pemrograman aplikasi mobile.
2. Membuat aplikasi mobile berbasis Android yang dapat mengamankan pesan singkat atau SMS.
3. Sebagai salah satu syarat untuk dapat menyelesaikan jenjang pendidikan Strata-1 di STMIK AMIKOM Yogyakarta.

1.5 Maksud dan Manfaat Penelitian

Manfaat yang ingin dicapai penulis dalam penelitian dan penyusunan skripsi ini adalah :

a) Bagi Penulis

Penulis dapat menerapkan ilmu yang diperoleh selama mengikuti perkuliahan dan diharapkan aplikasi yang dibuat bisa bermanfaat untuk banyak orang dalam membantu mengamankan pesan mereka. Serta

sebagai syarat untuk menyelesaikan pendidikan Strata-1 Teknik Informatika di STMIK AMIKOM Yogyakarta.

b) Bagi Pengguna

Membantu pengguna untuk mengamankan pesan singkat atau SMS mereka tanpa takut disadap oleh pihak yang tidak bertanggungjawab.

c) Bagi Pembaca

Penelitian ini dapat dijadikan referensi untuk pengembangan aplikasi berbasis android ataupun penelitian selanjutnya.

1.6 Metode Penelitian

Peneliti menjabarkan cara-cara memperoleh data-data yang digunakan untuk kebutuhan penelitian.

Pada penyusunan skripsi yang berjudul "Implementasi Hybrid Cryptosystem Menggunakan Algoritma RSA, 3DES dan MD5 pada Aplikasi SMS Berbasis Android" ini, penulis mengumpulkan data menggunakan beberapa langkah-langkah sebagai berikut:

a) Study Pustaka/Literatur

Untuk mendukung pengembangan aplikasi ini, penulis melakukan studi pustaka/literatur yaitu studi yang dilakukan dengan cara mencari dan membaca literatur serta karya-karya ilmiah tentang android, ilmu kriptografi, serta data-data yang berhubungan dengan sumber informasi lain sebagai acuan dalam pelaksanaan kegiatan dan penyusunan laporan.

b) Perancangan Sistem

Tahap perancangan sistem merupakan langkah awal yang dilakukan untuk membuat tampilan aplikasi meliputi perancangan *UML* dan *user interface*.

c) Pembuatan Aplikasi

Sistematika pembuatan aplikasi disesuaikan dengan perancangan sistem yang telah dilakukan pada tahap diatas. Tahapan ini meliputi *coding*, implementasi algoritma, serta implementasi hasil-hasil yang diperoleh dari referensi.

d) Pengujian Aplikasi

Pengujian aplikasi dilakukan pada dua *platform* yaitu Laptop/Komputer dan Telepon seluler. Pengujian pada Laptop/Komputer dilakukan dengan menggunakan *software* Eclipse dan emulator android SDK, sedangkan pengujian dengan *smartphone* Android.

e) Analisis dan Evaluasi

Melakukan pengujian aplikasi, sehingga memperoleh data-data yang diperlukan untuk mengetahui apakah aplikasi tersebut berjalan sesuai dengan tujuan dan perancangan sistem yang dibuat. Setelah itu kita dapat mengetahui kekurangan dari aplikasi tersebut yang perlu dibenahi.

1.7 Sistematika Penulisan

Penyusunan dan penulisan skripsi ini meliputi lima bab dengan perincian sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisi pembahasan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan. Yang merupakan bagian pengantar dari pokok permasalahan yang dibahas dalam penyusunan skripsi ini.

BAB II : LANDASAN TEORI

Bab ini bersifat teoritis, yaitu membahas tentang teori-teori yang berhubungan dengan perancangan aplikasi dan ilmu kriptografi.

BAB III : ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis sistem, perancangan sistem dan *interface* atau tampilan aplikasi.

BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Bab ini akan membahas bagaimana aplikasi digunakan dan apakah berfungsi dengan baik. Serta memaparkan hasil dari tahapan-tahapan penelitian.

BAB V : PENUTUP

Bab ini akan membahas kesimpulan yang didapat dari keseluruhan laporan dan perancangan aplikasi, serta kritik dan saran yang berguna baik bagi penulis maupun penulis lain yang berminat menjadikan skripsi ini sebagai referensinya.