BAB I
PENDAHULUAN

1.1 Latar Belakang

Layanan pesan singkat atau Surat masa singkat yang biasa disingkat SMS (*Short Message Service*), sebuah layanan yang dilaksanakan dengan sebuah ponsel untuk mengirim atau menerima pesan-pesan pendek,. Pengirim pesan instan akan mengirimkan teks melalui perangkat yang terhubung dengan suatu jaringan.

Perkembangan Teknologi dan Informasi yang maju pesat beberapa tahun ini menghasilkan sebuah ponsel dengan kemampuan komputasi dan konektifitas yang lebih maju yang biasa di sebut Smartphone. *Smartphone* menawarkan layanan yang lebih banyak dan lebih menarik dibanding ponsel biasa dan salah satunya adalah aplikasi *Chatting*. dengan kelebihan yang dimilikinya seperti biaya yang lebih murah dan tampilan pesan yang lebih menarik dari SMS, chatting mampu menarik banyak pengguna smartphone untuk mulai meninggalkan layanan SMS. Namun pada saat ini layanan SMS masih menjadi pilihan utama para pengguna ponsel untuk mengolah pesan pendek.

Isi yang di sampaikan di dalam pesan tersebut merupakan Data atau Informasi Pribadi dari para pengguna. Pengguna Layanan SMS ini akan merasa sangat dirugikan jika data yang mereka rahasiakan dapat dibaca pihak-pihak tertentu. Hal ini disebabkan masih ada beberapa celah dari sistem kemana data yang digunakan oleh operator seluler saat ini , Oleh karena itu, diperlukan adanya suatu mekanisme baru yang dapat menjaga kerahasiaan data tersebut. Metoda yang digunakan untuk mengamankan data ada bermacam – macam. Masing – masing metoda memiliki kelebihan dan kekurangan, salah satu dari metoda tersebut adalah kriptografi

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matemetika yang berhubungan dengan aspek keamanan informasi. Salah satu metoda kriptografi yang dianggap sebagai algoritma block cipher yang terbaik dan teraman yang tersedia untuk publik sampai saat ini adalah metoda kriptografi IDEA *(International Data Encryption Algorithm*).

Metoda IDEA diperkenalkan pertama kali oleh Xuejia Lai dan James Massey pada tahun 1990 dengan nama PES (*Proposed Encryption Standard*). Tahun berikutnya, setelah Biham dan Shamir mendemonstrasikan *cryptanalysis* yang berbeda, sang penemu memperkuat algoritma mereka dari serangan dan algoritma hasil pengubahan tersebut diberi nama IPES (*Improved Proposed Encryption Algorithm*). Kemudian pada tahun 1992, IPES diganti namanya menjadi IDEA (*International Data Encryption Algorithm*). Metoda IDEA ini menggunakan beberapa operasi dasar, seperti operasi logika *XOR* (*Exclusive – OR*), operasi perkalian mod $2^{16} + 1$ (*multiplication modulo* $2^{16} + 1$) dan operasi penambahan mod 2^{16} (*addition modulo* 2^{16}). Metoda ini terdiri dari 8 putaran (*round*) dan menggunakan 64 *bit plaintext* dengan panjang kunci sebesar 128 *bit*.

Berdasarkan uraian di atas, penulis bermaksud untuk mengambil tugas akhir (skripsi) dengan judul "Implementasi Kriptografi IDEA (International Data Encryption Algorithm) Sebagai Pengaman SMS Pada Smart Phone Berbasis Android)".

1.2 Rumusan Masalah

Tugas akhir ini menelaah metode dasar enripsi-dekripsi kriptografi IDEA dan mengimplementasikan sitem kriptografi IDEA pada pengiriman SMS di *Smartphone* berbasis android. .

1.3 Tujuan Tugas Akhir

Tugas akhir ini bertujuan untuk mempelajari dan megimplementasikan kriptografi IDEA sebagai kriptografi simetrik pada *Smartphone* berbasis Android dalam pengiriman SMS agar setiap SMS yang dikirimkan dapat dijaga kerahasiaan dan integritasnya. Dengan mengimplementasikan kriptografi IDEA, SMS yang dikirimkan tidak dapat dibaca, dimengerti, atau diubah oleh pihak lain selai pengirim dan pihak penerima yang dituju.

1.4 Metodologi Penetian

1.4.1 Studi Pustaka

Tugas akhir diawali dengan mempelajari literatur yang bergubungan dengan kriptografi IDEA dan OS android, artikel-artikel mengenai implementasi kriptografi IDEA dan pembuatan aplikasi pada OS Android.

1.4.2 Implementasi dan Uji Coba Aplikasi

Tugas akhir dilanjutkan dengan mengimplementasikan kriptografi IDEA pada OS Android. Hasil implementasi diuji coba pada sebuah emulator Android SDK manager pada program eclipse untuk melihat performa, waktu, bentuk pesan yang terenktipsi , dan integritas data dari pengiriman SMS yang menggunakan hasil implementasi.

1.5 Sistematika Penulisan

Bab 1 Pendahuluan

Bab ini berisi latar belakang, rumusan masalah dan ruang lingkup, tujuan penelitian, metode penelitian, dan sistematika penelitian.

Bab II Landasan Terori

Memaparkan teori-teori yang didapat dari sumber-sumber yang relevan untuk digunakan sebagai panduan dalam penelitian serta penyusunan Skripsi.

Bab III Analisis Sistem dan Perancangan

Menjelaskan tentang gambaran sistem, deskripsi dari hasil analisis sistem yang akan dijadikan sebagai petunjuk untuk perancangan pada tahapan berikutnya dan Berisi tentang Perancangan Sistem, Perancangan Data, Perancangan Arsitektural, Perancangan Prosedural dan Perancangan Antarmuka.

Bab IV Implementasi Dan Pembahasan

Berisi tentang rancangan, desain, proses instalasi, pembuatan dan hasil akhir dari sistem..

Bab V Penutup

Mengemukakan kesimpulan yang diambil dari hasil penelitian dan penulisan Skripsi ini, serta saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang.