1 Pendahuluan

1.1 Latar Belakang

SMS Banking merupakan media transaksi yang sampai saat ini sangat diminati oleh nasabah Bank. SMS Banking memberikan kemudahan untuk mendapatkan berbagai fasilitas yang diberikan dari pihak Bank. Macam-macam fasilitas tersebut contohnya pembayaran listrik, transfer uang, pembelian barang, pembelian pulsa, dan lain-lain.

Jika dilihat dari kebutuhan fungsionalitas SMS Banking maka SMS Banking berisi data yang relatif pendek tetapi mengandung informasi yang sangat rahasia. Oleh karena itu, SMS Banking harus mendapatkan perhatian lebih pada aspek keamanan. SMS merupakan media komunikasi yang saat ini masih rentan terhadap ancaman keamanan salah satunya *confidentiality* data, yaitu data bisa dibaca oleh *interceptor* bahkan SMS *provider*. Salah satu cara untuk menyembunyikan data agar tidak dapat dibaca oleh pihak ke-tiga/*interceptor* adalah enkripsi data.

Upaya dukungan keamanan data pernah diberikan oleh operator GSM yaitu menggunakan metode enkripsi data menggunakan algoritma A5. Namun, A5 sudah mampu dipecahkan oleh pihak *interceptor*[2][3]. Oleh karena itu dibutuhkan algoritma enkripsi lain yang mampu melakukan enkripsi data dengan baik.

Pada tugas akhir ini akan diterapkan algoritma Elgamal untuk enkripsi SMS. Algoritma Elgamal merupakan algoritma enkripsi asimetris yang berarti bahwa kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk melakukan dekripsi pesan. Kekuatan Algoritma Elgamal ada pada Permasalahan Logaritma Diskrit yang sampai saat ini belum ada solusi untuk memecahkan kekuatan enkripsi tersebut dengan cepat[1][6]. Keunikan algoritma Elgamal dibandingkan dengan algoritma enkripsi asimetris lainnya adalah hasil enkripsi pesan dapat berbeda untuk plainteks yang sama dengan menggunakan kunci publik yang sama[1][6][9]. Keunikan tersebut merupakan kelebihan yang dimiliki oleh algoritma Elgamal.

Algoritma Elgamal saat ini digunakan dalam PGP (*Pretty Good Privacy*) untuk manajemen pengamanan *Email* yang melakukan enkripsi *secret key* dari *symmetric encryption scheme*[8], Digital Signature pada SmartCard, enkripsi authentikasi pada Eliptic Curve Cryptography[16], dll. Selain itu, Elgamal digunakan dalam GnuPG *(GNU Privacy Guard)*

dalam menerapkan hybrid cryptosystem untuk enkripsi *secret key*. Pada umumnya *secret key* yang dimiliki oleh *symmetric encryption scheme* berukuran kecil, yaitu 16 Byte hingga 32 Byte[15]. Oleh karena itu, algoritma Elgamal dipilih untuk enkripsi data sesuai dengan tingkat keamanan yang didapatkan dari Algoritma Elgamal serta sesuai dengan konten transaksi dalam SMS Banking yang menggunakan data relatif kecil (40-50) Byte.

Aplikasi enkripsi SMS akan diimplementasikan pada platform / Sistem Operasi Android. Android dipilih sebagai platform aplikasi karena Android merupakan sistem operasi Mobile yang Open Source. Selain itu, Android merupakan platform yang masih tergolong baru dan sudah cukup banyak beredar di pasaran [11].

1.2 Perumusan Masalah

Perumusan masalah yang ditinjau adalah bagaimana membangun Sistem Enkripsi SMS menggunakan algoritma Elgamal pada Sistem Operasi Android sehingga pesan (SMS) yang dikirimkan melalui kanal komunikasi dapat disembunyikan.

1.3 Tujuan

Adapun tujuan dari Tugas Akhir adalah sebagai berikut.

a. Mengimplementasikan Algoritma Elgamal untuk enkripsi SMS pada Sistem Operasi Android.
b. Melakukan pengukuran lama pembangkitan kunci, enkripsi dan dekripsi SMS.
c. Melakukan pengukuran penggunaan memory untuk proses enkripsi maupun dekripsi.
d. Melakukan pengukuran perubahan ukuran file (teks) setelah proses enkripsi.

1.4 Metodologi Penyelesaian Masalah

Metodologi penyelesaian Masalah yang digunakan adalah:

a. Studi Literatur

   Merupakan tahap dan cara mencari informasi pendukung untuk menyelesaikan permasalahan. Pada tahap ini akan dilakukan pencariann referensi-referensi yang berkaitan dengan enkripsi Elgamal, SMS, aplikasi SMS pada Android, cara pengukuran waktu proses pada aplikasi android, cara pengukuran penggunaan memory pada aplikasi

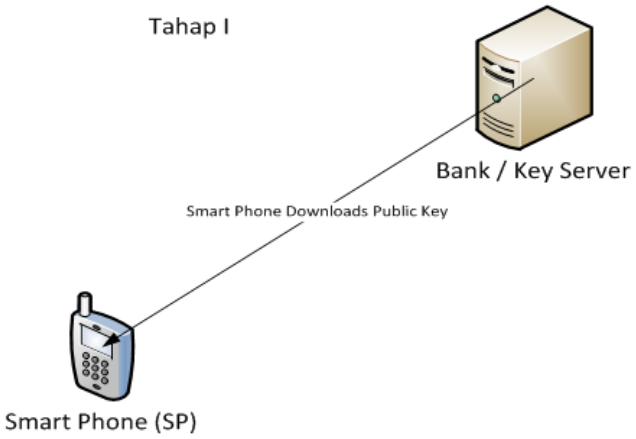
Android. Dari sini maka akan dapat ditentukan cara melakukan pengujian terhadap aplikasi yang sudah dibuat.

b. Analisis Kebutuhan

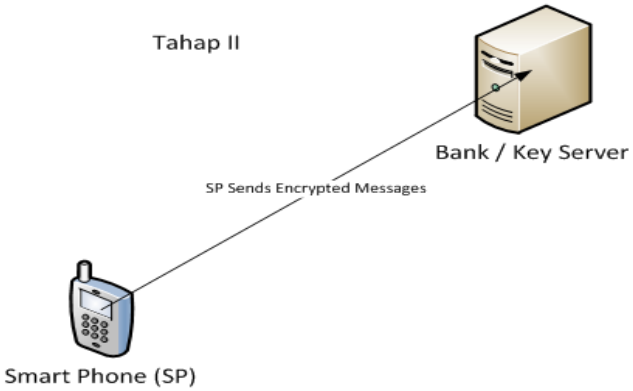
Pada tahap ini akan dilakukan analisis kebutuhan terhadap perancangan aplikasi SMS pada Android dengan menggunakan Algoritma enkripsi Elgamal agar sistem yang dibuat mampu menyembunyikan pesan (*Data Confidentiality*) yang dikirimkan melalui kanal komunikasi. Aplikasi SMS juga mampu mendekripsikan pesan yang terenkripsi (yang tiba di penerima) tersebut sehingga dapat dibaca kembali oleh pelanggan.

c. Perancangan Sistem

Pada tahap ini dilakukan perancangan Sistem dengan menyediakan *device / hardware* serta menentukan sistem operasi Android yang digunakan oleh *device / hardware* tersebut. Sistem operasi Android yang akan digunakan adalah Android 2.2 Froyo. Aplikasi akan dibuat menggunakan bantuan Simulator Android SDK (Software Development Kit) sebagai media perantara agar programmer mampu meletakkan program ke dalam *hardware*/*device* mobile Android. Pada saat mengirim pesan aplikasi akan melakukan enkripsi pesan SMS terlebih dahulu sedangkan pada saat menerima aplikasi akan mendekripsi pesan yang tiba di penerima. Enkripsi pesan dilakukan dengan menggunakan kunci publik yang dimiliki oleh *receiver*. Jika pengirim tidak mempunya kunci publik milik penerima maka pengirim harus mengambil kunci publik penerima yang terdapat pada *Key Server*. Pertukaran kunci dapat dilakukan dengan cara mengakses *Key Server*. *Key Server* dibuat dengan tujuan dapat mensimulasikan pertukaran kunci.



Gambar 1-1 Desain Rencana Arsitektur Sistem



Gambar 1-2 Desain Rencana Arsitektur Sistem Tahap II

Perancangan Sistem di atas terbagi menjadi dua tahap. Tahap I adalah tahap mendapatkan public key dari Bank. Tahap II adalah tahap enkripsi kunci oleh client menggunakan public key yang sudah diperoleh. Tahap satu dilakukan cukup sekali untuk satu bank sedangkan Tahap II dilakukan pada setiap melakukan transaksi. Enkripsis pesan dilakukan ketika pengiriman pesan dari client ke bank sedangkan dari pengiriman pesan dari bank ke client tidak dilakukan enkripsi.

d. Testing dan Analisis Hasil

Pada tahap ini akan dibuat sekenario pengujian. Sekenario pengujian akan dilakukan dengan menguji keberhasilan sistem sesuai dengan kebutuhan (*requirement*) yang telah ditentukan. Selain itu, akan dilakukan pengukuran waktu enkripsi/dekripsi dan pengukuran penggunaan memory pada saat enkripsi/dekripsi pesan serta mengukur besar ukuran pesan sebelum dan setelah enkripsi.

Analisis akan dilakukan dengan melihat hubungan antara besar file dengan waktu enkripsi /dekripsi. Selain itu, akan dilihat bagaimana hubungan antara besar ukuran pesan dengan penggunaan memory pada saat enkripsi dan dekripsi. Dan yang terakhir akan dilihat bagaimana hubungan antara ukuran pesan sebelum dan sesudah dilakukan enkripsi.

e. Penyusunan Laporan

Pada tahap ini dilakukan penyusunan laporan terhadap penelitian yang telah dilaksanakan yang tentunya akan menghasilkan suatu kesimpulan.

1.5 Batasan Masalah

a. Sistem Enkripsi SMS yang dibuat hanya menangani Confidentiality Data.
b. Teknologi yang digunakan adalah Sistem Operasi Android pada perangkat komunikasi Mobile.
c. Asumsi bilangan prima yang digunakan adalah bilangan prima aman.
d. Dalam pembuatan tugas akhir tidak melakukan pengujian penyadapan SMS terenkripsi.
e. Kondisi Jaringan infrastruktur SMS tidak pada kondisi sibuk.
f. Sistem enkripsi SMS hanya diterapkan pada teknologi GSM.

1.6 Hipotesis

Hasil enkripsi pesan menggunakan algoritma Elgamal akan berubah-ubah untuk pesan / SMS dan kunci publik yang sama. Hal tersebut disebabkan oleh nilai acak yang dibangkitkan pada sisi pengirim yang digunakan untuk melakukan enkripsi pesan. Dengan hasil enkripsi yang berubah-ubah pada setiap pengiriman pesan tersebut maka akan mampu mengurangi peluang attacker dan sekaligus menambah tingkat kesulitan *Interceptor* (penyadap) untuk melakukan dekripsi pesan. Algoritma Elgamal kemungkinan cocok diterapkan pada enkripsi SMS karena Algoritma Elgamal sering digunakan untuk enkripsi data yang relatif kecil, misal : untuk enkripsi kunci simetrik, enkripsi data authentikasi, dll.