1. Pendahuluan

1.1 Latar Belakang

Sejak tahun 1990-an, internet berkembang pesat ke seluruh dunia karena semakin mudahnya akses informasi ke jejaring internet dengan menggunakan teknologi WWW (*World Wide Web*). Saat ini, internet telah menjadi bagian dari kehidupan sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk pribadi. Namun di sisi lain, ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut.

Oleh karena penggunaan internet yang sangat luas seperti perdagangan, bank, industri, dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia, maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Selain untuk merahasiakan data, menyandikan isi informasi juga memliki tujuan untuk melindungi privasi masing-masing anggota masyarakat yang terhubung ke internet.

Mulanya keamanan penyandian ditentukan dengan menjaga kerahasiaan algoritmanya. Algoritma ini dinamakan algoritma *restricted*, dimana algoritma ini digunakan oleh sekelompok orang untuk bertukar pesan satu sama lain. Tetapi algoritma ini tidak efisien, karena setiap kali ada anggota kelompok keluar, maka algoritma tersebut harus diganti. Untuk mengatasi masalah di atas digunakan metode penyandian dengan penggunaan kunci. Metode ini tidak menumpukkan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Algoritmanya dapat diketahui, digunakan, dan dipelajari oleh siapapun.

Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia.

Algoritma ElGamal merupakan salah satu algoritma kriptografi kunci yang dibuat oleh Taher ElGamal pada tahun 1984. Algoritma ini pada umumnya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga bisa digunakan untuk enkripsi dan dekripsi. Alasan digunakan algoritma kriptografi ElGamal dalam tugas akhir ini karena tingkat keamanan pada algoritma ini didasarkan atas masalah logaritma diskrit, apabila digunakan bilangan prima dan logaritma diskrit yang besar, maka upaya untuk menyelesaikan masalah logaritma diskrit ini menjadi sia-sia dan dirasakan tidak sesuai dengan isi informasi yang ingin diperoleh.

Windows XP dan Ubuntu merupakan sistem operasi yang banyak digunakan saat ini. Kedua sistem operasi ini memiliki kernel yang berbeda sehingga performa aplikasi yang berjalan di atasnya juga berbeda. Beberapa aplikasi dapat berjalan lebih baik di Windows XP, begitu juga sebaliknya di Ubuntu. Dalam tugas akhir ini akan digunakan sistem operasi Windows XP dan Ubuntu untuk mengukur performa algoritma ElGamal jika diimplementasikan di sistem operasi yang berbeda.

1.2 Rumusan Masalah

Yang menjadi rumusan masalah dalam tugas akhir ini adalah:

1. Bagaimana mengimplementasikan algoritma ElGamal dalam sebuah program komputer.
2. Bagaimana performa algoritma ElGamal jika diimplementasikan pada sistem operasi yang berbeda.

Yang menjadi batasan masalah pada tugas akhir ini meliputi:

1. File yang digunakan untuk proses enkripsi/dekripsi berupa file teks dengan ekstensi .txt.
2. Sistem operasi yang digunakan adalah Windows XP dan Ubuntu.
3. Tidak membahas mengenai cara memecahkan mekanisme penyandian.

1.3 Tujuan Tugas Akhir

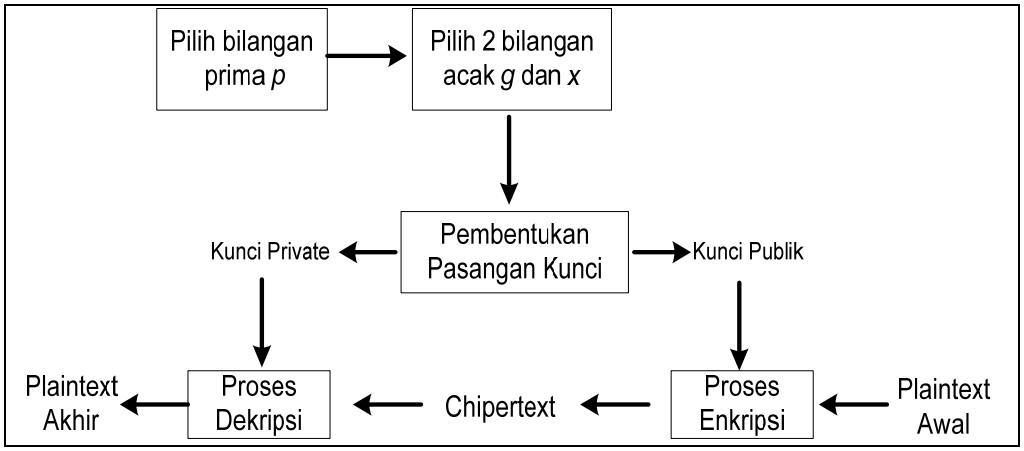
Selain untuk memenuhi persyaratan dalam rangka menyelesaikan pendidikan Program Sarjana Jurusan Teknik Informatika Institut Teknologi Telkom, penyusunan skripsi ini bertujuan untuk:

1. Mengimplementasikan algoritma ElGamal ke dalam sebuah program komputer.
2. Menganalisis performa algoritma ElGamal jika diimplementasikan pada sistem operasi yang berbeda dengan melihat waktu yang dibutuhkan untuk proses pembentukan kunci, proses enkripsi, dan proses dekripsi, serta kebutuhan memori setelah proses enkripsi.

Hipotesa awal dari implementasi algoritma ElGamal pada sistem operasi Windows XP dan Ubuntu dilihat dari parameter waktu adalah relatif sama, karena baik Windows XP maupun Ubuntu menyediakan sarana yang sama untuk pembangkitan bilangan acak, yaitu *Application Programming Interface* (API) pembangkit bilangan acak. Windows XP dan Ubuntu menggunakan API pembangkit bilangan acak yang sama yaitu file <stdlib.h>. Sedangkan jika dilihat dari parameter kebutuhan memori setelah proses enkripsi akan relatif sama, karena tiap karakter dalam plainteks akan diubah menjadi pasangan (γ, δ) dalam cipherteks.

1.4 Metodologi Penyelesaian Masalah

1. Studi literatur mengenai algoritma ElGamal melalui beberapa buku, paper maupun situs internet yang berhubungan dengan algoritma ElGamal.
2. Perancangan terhadap program komputer yang akan dibuat.



Gambar 1-1 Gambaran umum proses penyandian data menggunakan algoritma kriptografi ElGamal

a. Pilih sembarang bilangan prima *p*

b. Pilih 2 bilangan acak, *g* dan *x* dimana $g < p$ dan $1 \leq x \leq p$-2

c. Pembentukan pasangan kunci

d. User memasukkan *plaintext* yang akan dienkrip

e. Proses enkripsi menggunakan kunci publik.

f. Hasil proses enkripsi berupa *chipertext*.

g. Untuk memperoleh *plaintext* kembali, dilakukan dekripsi terhadap *plaintext* menggunakan kunci *private*.

3. Mengimplementasikan perancangan yang telah dibuat dengan membangun aplikasi algoritma ElGamal menggunakan bahasa C.
4. Melakukan pengujian dengan menjalankan algoritma di sistem operasi Windows XP dan Ubuntu menggunakan ukuran file yang berbeda-beda.
5. Penarikan kesimpulan terhadap pengujian yang telah dilakukan dan pembuatan laporan.

1.5 Sistematika Penulisan

Struktur pembahasan tugas akhir ini disusun sebagai berikut:

BAB 1 Pendahuluan

Bab ini berisi latar belakang masalah, perumusan masalah, batasan masalah, tujuan tugas akhir, metodologi penyelesaian masalah, sistematika penulisan.

BAB 2 Landasan Teori

Membahas dasar teori yang berhubungan dengan pengertian umum kriptografi, pengamanan data menggunakan algoritma kriptografi ElGamal, dan sistem operasi.

BAB 3 Perancangan

Bab ini akan membahas proses perancangan aplikasi pengamanan data menggunakan algoritma kriptografi ElGamal.

BAB 4 Implementasi dan Analisis Hasil Uji Coba

Membahas tentang analisis dari hasil pengujian ataupun percobaan pada implementasi algoritma kriptografi ElGamal.

BAB 5 Kesimpulan dan Saran

Pada bab ini akan menjelaskan kesimpulan dan saran sebagai hasil dari analisa dan implementasi algoritma kriptografi ElGamal.