BAB I
PENDAHULUAN

1.1 Latar Belakang

Dunia teknologi saat ini semakin berkembang pesat hingga sekarang. Teknologi yang saat ini berkembang pesat justru membuat *cybercrime* menjadi lebih agresif dalam melakukan tidak kejahatan terutama di dunia maya. Tentu kejahatan dalam dunia maya merupakan hal yang sangat merugikan baik bagi pengguna Internet maupun penyedia jasa Internet. Banyaknya informasi-informasi penting baik yang dipublikasikan maupun yang bersifat rahasia. Namun kenyataannya banyak kasus pencurian data atau penyadapan data yang sangat rahasiapun bisa dibobol oleh pihak yang tidak bertanggung jawab yang biasa dikenal sebagai cybercrime. Untuk mengamankan data penting yang berupa informasi tersebut adalah kriptografi.

Kita tidak meyadari bahwa kita sekarang banyak dilingkupi oleh kriptografi. Mulai dari percakapan telpon genggam, akses Internet, sampai aktivitas transaksi di ATM telah menggunakan kriptografi. Sangat penting kriptografi untuk keamanan Informasi, sehingga jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka tidak akan bisa dipisahkan dari kriptografi. Ilmu kriptografi juga telah mengalami perkembangan yang cepat, hal ini dikarenakan perkembangan teknologi informasi yang juga semakin cepat terutama pada aspek keamanan data.

Email merupakan layanan terpenting yang diberikan internet. Mayoritas masyarakat menggunakan internet untuk membaca dan mengirim *email*. *Email* mengubah mekanisme komunikasi sehingga orang-orang dapat berkomunikasi jarak jauh dalam waktu yang relatif singkat.

Kriptografi juga digunakan dalam proses pengiriman *Email*. Jika *email* dikirim melewati jaringan *public* maka tingkat keamannya sangat beresiko. Teknik- teknik pencurian informasi dari sebuah *email* ini semakin canggih dari hari ke hari. Salah satunya adalah serangan *Man – In – The Middle*. Kriptografi akan sangat membantu memberikan keamanan informasi *email* kita. Walaupun attacker atau Man – In – The Middle berhasil mendapatkan teks yang kita kirim namun tidak bisa mendapatkan informasi yang akurat karena teks yang didapat sudah ter-enkripsi sebelumnya. Sedangkan *Chiperteks* yang didapat hanya bisa dibuka oleh pihak yang memiliki *kunci private* (Kunci untuk dekripsi).

Masalah yang sampai saat ini marak terjadi yaitu kasus *phishing mail* . *Email Phising* adalah upaya memperoleh atau "mengelabui" informasi agar pelaku kejahatan di dunia maya dapat mencuri uang atau identitas sesorang (target *phising*). *Email* tersebut terlihat sama dengan *email* asli dari perusahaan ternama seperti paypal, bank, web olshop, game, bahkan sosial media. Cara pelaku melakukan aksinya, pelaku akan mengirimkan informasi ke target yang berisi notifikasi berupa alasan akan memperbarui informasi pribadi maupun keuangan atau mengkonfirmasi sandi dari target *phishing*.

Kaspersky (2015) , Dari data kapersky lab yang penulis dapatkan mulai tahun 2011 sampai 2015 memaparkan bahwa di tahun 2011 hingga 2012 angka pengguna *email* yang terserang phishing *email* mencapai 19.90 jt sedangkan di tahun 2012 hingga 2013 mencapai 37.30 jt. Bank adalah salah satu target utama para phishier, 20.64% ditahun 2011-2013, 16.8% ditahun 2014-2015. Sedangkan Negara yang menjadi target utama saat ini adalah Brazil dengan persentase 18.28% tahun 2015. Sedangkan Yahoo menjadi top target daripada sang rival yakni google dan facebook dengan persentase 25.10% tahun 2015.

Permasalahan tersebut dapat diatasi dengan proses enkripsi. Salah satu enkripsi yang cukup dikenal adalah dengan metode enkripsi ELGamal. Metode enkripsi ELGamal ini akan memberikan *public key* dan *private key* yang digunakan dalam proses Enkripsi dan Dekripsi. Dalam proses pembentukan kunci public dan rahasia, dibutuhkan suatu bilangan prima yang bernilai besar agar menjadi aman. Aplikasi *email* ini dibangun pada perangkat desktop JAVA. Sehingga diharapkan aplikasi dekstop ini dapat menjaga kerahasiaan informasi-informasi penting, terutama para nasabah bank yang awam akan kasus *phising mail* yang telah memakan banyak korban.

Berdasarkan latarbelakang yang telah dijabarkan di atas, maka penulis mengangkat skripsi dengan judul **"Implementasi Algoritma Kriptografi ELGamal untuk keamanan pengiriman E-mail berbasis JAVA".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian/perancangan ini. Adapun pokok permasalahan dalam penelitian ini adalah Bagaimana membuat dan mengimplementasikan algoritma kriptografi ELGamal untuk mengenkripsi pesan maupun document yang akan di kirim melalui *email* pada aplikasi Java.

1.3 Batasan Masalah

Agar masalah yang diteliti tidak menyimpang maka diperlukan suatu batasan masalah. Dalam suatu penelitian ini peneliti membatasi masalah yang diteliti, yaitu pada aplikasi pengamanan pengiriman *email* enkripsi dan dekripsi pesan dengan algoritma kriptografi ELGamal. Adapun batasan masalah pada penelititan ini adalah sebagai berikut :

1. Aplikasi ini berbasis *desktop Windows*.
2. Aplikasi ini hanya menggunakan algoritma kriptografi ELGamal saja dalam proses enkripsi dekripsi pesan dan *document*.
3. Inputan ke apliksi berupa teks tertulis dan document.
4. Peneliti tidak berfokus sepenuhya pada pembuatan program pendukung aplikasi tetapi pada implementasi dan hasil analisa dari program yang dibuat.
5. Sistem operasi yang digunakan peneliti dalam pembuatan aplikasi kriptografi ELGamal dengan menggunakan Windows 8.1.
6. Pembuatan program pendukung aplikasi kriptografi ELGamal menggunakan bahasa JAVA.

7. Algoritma kriptografi, bahasa pemrograman, sistem operasi, dan program pendukung selain yang disebutkan tidak dibahas dan tidak digunakan dalam penelitian ini.

1.4 Maksud dan Tujuan Penelitian

Untuk menunjang penguasaan ilmu yang telah diberikan oleh lembaga pendidikan Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta, yang berorientasi pada Teknologi Informasi dan Komputerisasi. Adapun maksud dan tujuan yang ingin dicapai dari penelitian ini adalah :

1.4.1 Internal

Pengertian tujuan internal yang dimaksud adalah dilihat dari sisi penulis. Dalam hal ini penulis sebagai Mahasiswa Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta adalah sebagai berikut :

1. Sebagai prasyarat untuk memperoleh gelar Strata-1 Jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Menerapkan ilmu teoritis yang didapat selama mengikuti pendidikan di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
3. Sebagai tolak ukur, sejauh mana ilmu yang didapat diperkuliahan dapat diterapkan kedalam lingkungan permasalahan yang sebenarnya dengan cara terlibat langsung dalam proses pembuatan aplikasi.

4. Memperluas serta meningkatkan kemampuan mahasiswa sebagai bekal untuk memasuki dunia kerja.

1.4.2 Eksternal

Bagi masyarakat luas dan dunia pendidikan pada umumnya penelitian ini mempunyai tujuan sebagai berikut :

1. Adanya implementasi dan hasil analisa yang mampu ditunjukkan sebagai bukti bahwa algoritma kriptografi ELGamal mampu digunakan sebagai aplikasi yang bisa merahasiakan pesan *email* dan dokumen yang sulit dipecahkan dengan perhitungan tanpa bantuan komputer.
2. Mengahasilkan sebuah program aplikasi berbasis *desktop* yang berfungsi untuk mengenkripsi dan dekripsi pesan *email* serta dokumen dengan algoritma kriptografi ELGamal berbasis JAVA.
3. Sebagai bahan penelitian yang dapat dikembangkan dan diperbaiki pada penelitian berikutnya.

1.5 Manfaat Penelitian

Manfaat yang akan didapat dari penelitian ini adalah sebagai berikut :

1. Dapat memberikan perlindungan terhadap informasi pesan maupun *document* agar tidak mudah untuk diakses oleh pihak-pihak yang tidak bertanggung jawab.
2. Pengguna aplikasi tidak perlu khawatir lagi terhadap *email phising* yang sengaja ingin mencuri data dan informasi penting.

3. Dapat digunakan sebagai bahan kajian untuk mengembangkan teknologi informasi terutama faktor yang berhubungan dengan keamanan.

1.6 Metode Penelitian

Penulis melakukan beberapa metode penelitian dan mengumpulkan data untuk memperoleh jawaban atas permasalahan yang penulis ungkapkan. Adapun metode-metode yang penulis lakukan adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode pengumpulan informasi dan data yang digunakan dalam penelitian ini diantaranya:

1.6.1.1 Metode Studi Kepustakaan

Untuk mendukung perancangan aplikasi ini penulis menggunakan metode studi kepustakaan sebagai referensi. Pustaka yang digunakan antara lain *journal*, *website* atau penelitian sebelumnya yang berkaitan dengan penelitian ini.

1.6.1.2 Metode Browsing

Metode *browsing* yaitu teknik pengumpulan rujukan yang bersumber dari internet dengan mengunjungi situs yang berhubungan dengan penelitian ini

1.6.1.3 Metode Wawancara

Metode wawancara yaitu melakukan tanya jawab langsung dengan pihak yang terkait dengan masalah yang diteliti.

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah analisis SWOT.

1.6.2.1 Analisis SWOT

Analisis SWOT adalah singkatan dari (*Strengths, Weakness, Opportunities, Threats*) yaitu penganalisa kekuatan, kelemahan, peluang serta ancaman dalam hasil penelitian ini.

1.6.2.2 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem adalah beberapa kebutuhan dalam sistem untuk mendukung jalannya proses pembuatan dan kinerja aplikasi yang dibuat.

1.6.2.3 Analisis Kelayakan Sistem

Analisis kelayakan adalah untuk menentukan layak tidaknya aplikasi yang dibuat. Analisis kelayakan yang digunakan adalah dari segi teknologi, operasional, dan hukum.

1.6.3 Metode Perancangan

Metode perancangan yaitu dengan menggunakan perancangan UML (*Unified Modelling Language*), *flowchart*, dan User Interface.

1.7 Sistematika Penulisan

Sistematika laporan disusun menggunakan dasar-dasar penulisan karya ilmiah. Metode ini dilakukan agar dalam penyusunan laporan menjadi lebih teratur dan mudah dipahami. Sistematika penulisan laporan pada skripsi adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang tinjauan pustaka dan dasar-dasar teori yang digunakan.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis sistem, analisis kebutuhan sistem, analisis kelayakan sistem dan perancangan sistem yang diusulkan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas mengenai hasil program yang akan diimplementasikan ke dalam perangkat computer.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dari keseluruhan laporan dan saran yang membangun untuk menambah kesempurnaan aplikasi.