BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam kehidupan sehari-hari manusia selalu bergantung pada teknologi informasi, baik dari hal kecil hingga ke suatu permasalahan yang rumit. Contoh teknologi informasi dalam kehidupan sehari-hari yaitu, *ATM, Internet Banking, Mobile Banking, Email, SMS, MMS, Chatting,* dan sebagainya. Kemajuan teknologi informasi memberikan banyak keuntungan bagi keberlangsungan kehidupan manusia, tetapi keuntungan yang ditawarkan oleh teknologi juga menimbulkan kejahatan seperti pencurian data. Sehingga perkembangan ilmu untuk mengamankan data semakin ditingkatkan agar pengguna teknologi selalu merasa aman. Berbagai cara dilakukan untuk menjaga keamanan data elektronik seperti menyembunyikan data tersebut, kemudian berupa regulasi yang dibuat pemerintah maupun penyandian data-data menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila disadap akan kesulitan untuk mengetahui dan memahami informasi yang sebenarnya.

Di Indonesia penggunaan teknologi informasi dilindungi oleh regulasi diantaranya Undang-undang ITE nomor 11 tahun 2008 yang memuat tentang peraturan penggunaan serta sanksi terhadap informasi dan transaksi elektronik sehingga dapat meminimalisir penyalahgunaan data informasi elektronik.

Informasi rahasia merupakan hal penting yang butuh suatu proteksi dan terjaga kerahasiaannya. Oleh karena itu maka tidak jarang muncul kejahatan-kejahatan yang dengan sengaja dilakukan oleh orang yang tidak bertanggung jawab. Dengan semakin banyaknya orang yang melakukan tindakan kriminal yang dengan sengaja melakukan pencurian data atau informasi rahasia dan merusaknya sehingga bisa merugikan pihak yang berhak akan informasi tersebut. Seiring dengan hal tersebut, maka dibuatlah suatu cara yang dapat memproteksi data, karena suatu kerahasiaan data atau informasi

begitu penting dan bersifat pribadi. Dengan banyaknya penggunaan teknik pengamanan digital bagi pengiriman dan penyimpanan data, masalah mendasar untuk melindungi kerahasiaan, keutuhan dan keasliannya memang perlu diperhatikan. Untuk meningkatkan keamanan salah satunya adalah dengan cara mengenkripsikan data tersebut. Belum banyaknya fitur pengenkripsian data sehingga menjadi peluang untuk dilakukan penelitian dalam tugas akhir atau skripsi ini.

Metode dalam meningkatkan keamanan salah satunya dalam penyandian data yang pertama kali dibuat masih menggunakan metode algoritma rahasia. Metode ini menumpukan pada kerahasiaan algoritma yang digunakan. Namun metode ini tidak efisien saat harus digunakan untuk berkomunikasi dengan banyak orang. Oleh karena, seseorang harus membuat algoritma baru apabila akan bertukar informasi rahasia dengan orang lain. Karena penggunanya merasa tidak efisien maka algoritma rahasia mulai ditinggalkan dan dikenalkan suatu metode baru yang disebut dengan algoritma kunci. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandiannya. Algoritmanya dapat diketahui dan dipelajari oleh siapapun. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Algoritma kunci yang dikenal dengan kriptografi telah melingkupi aspek kehidupan manusia saat ini. Begitu pentingnya kriptografi, saat berbicara tentang keamanan komputer orang tidak bisa memisahkannya dengan kriptografi.

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. (Ariwibowo, 2008). Salah satu fungsi kriptografi adalah kerahasian data, namun kriptografi yang sering dipakai justru dibobol oleh pihak yang tidak memiliki hak akses terhadap data rahasia. Sebut saja *brute force* dimana sang pembobol berusaha memecahkan data rahasia dengan kemungkinan-kemungkinan kunci yang dipakai dan masih banyak cara lain yang digunakan untuk mendapatkan pesan rahasia. (Kromodimoeljo, 2009)

Kriptografi sangat penting untuk dipelajari. Saat ini pembelajaran pun mulai dikemas secara lebih praktis dan menarik melalui media komputer karena komputer mampu menampilkan teks, warna, suara, video, gerak, gambar serta mampu menampilkan kepintaran yang dapat menyajikan proses interaktif. Media komputer dimanfaatkan dalam pembelajaran karena memberikan keuntungan-keuntungan yang tidak dimiliki oleh media pembelajaran lainnya yaitu kemampuan komputer untuk berinteraksi secara individu dengan mahasiswa.

Kriptografi adalah salah satu mata kuliah yang diajarkan di bidang ilmu komputer. Kriptografi harus ajarkan agar mahasiswa mengetahui cara-cara mengamankan data. Untuk mengatasi hal tersebut, diperlukan pembelajaran tentang pengamanan data yaitu menggunakan metode kriptografi kunci publik *El-Gamal*. Oleh karena itu ilmu untuk mengamankan data harus semakin ditingkatkan. Maka diperlukan pembelajaran tentang pengamanan data yaitu menggunakan metode kriptografi kunci publik *El-Gamal* kemudian membuat sebuah aplikasi pembelajaran bagi mahasiswa khususnya pembelajaran mata kuliah Kriptografi dan Proteksi Data.

Umumnya kriptografi terdiri atas dua operasi utama yaitu operasi enkripsi dan operasi dekripsi. Enkripsi adalah proses transformasi informasi atau *plaintext* menjadi bentuk lain sehingga isi data atau informasi yang sebenarnya tidak dapat dipahami atau bisa disebut *ciphertext*, hal ini dimaksudkan agar data atau informasi tetap terlindung dari pihak yang tidak berhak melihat atau menerimanya. Sedangkan dekripsi adalah proses kebalikan dari enkripsi, yaitu transformasi data ke dalam bentuk semula. Terdapat banyak teknik-teknik dalam memproteksi suatu data atau informasi dengan mengenkripsinya dengan algoritma tertentu.

Dalam penelitian ini akan digunakan salah satu metode algoritma kunci. Metode ini tidak menumpukkan keamanan algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Hingga saat ini ada beberapa algoritma kriptografi kunci publik yang sering digunakan, dan dalam penelitian ini juga akan menggunakan salah satunya yaitu Algoritma *El-Gamal*.

Algoritma *El-Gamal* merupakan salah satu dari algoritma kunci. Algoritma ini dikembangkan pertama kali oleh Taher El-Gamal pada tahun 1985. Algoritma ini pada mulanya digunakan untuk *digital signature*, namun kemudian dimodifikasi sehingga juga bisa digunakan untuk enkripsi dan dekripsi. Algoritma *El-Gamal* terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan *cipher* blok, yaitu melakukan proses enkripsi pada blok-blok *plaintext* dan menghasilkan blok-blok *ciphertext* yang kemudian dilakukan proses dekripsi dan hasilnya digabungkan. Keamanan algoritma ini terletak pada sulitnya menghitung logaritma diskrit. Pada bilangan modulo prima yang besar sehingga upaya untuk menyelesaikan masalah logaritma ini menjadi sangat sukar. Algoritma ini mempunyai kerugian pada *ciphertext*-nya yang mempunyai panjang dua kali lipat dari *plaintext*-nya. Akan tetapi, algoritma ini mempunyai kelebihan pada enkripsi. Untuk *plaintext* yang sama, algoritma ini memberikan *ciphertext* yang berbeda (dengan kepastian yang dekat) setiap kali *plaintext* dienkripsi.

Riyanto meneliti tentang pengamanan pesan rahasia menggunakan algoritma kriptografi *El-Gamal* atas grup penggandaan Zp*. Beliau menyimpulkan bahwa algoritma kriptografi asimetris seperti algoritma kriptografi *El-Gamal*, sangat baik untuk mengatasi masalah pada pendistribusian kunci. (Riyanto, 2007)

Sejauh perkembangan kriptografi, banyak pihak yang berusaha membongkar algoritma kriptografi itu sendiri. Oleh karena itu, solusi dari hal ini yaitu dilakukanlah penggabungan proteksi pesan dengan menggunakan kriptografi dan Steganografi. Steganografi yaitu ilmu untuk menyembunyikan atau menyisipkan data rahasia ke dalam sebuah gambar, dengan catatan tidak ada yang mengetahui ada suatu pesan rahasia selain pengirim dan penerima pesan. (Niswati, 2012)

Setelah ditinjau dari kelebihan dan kekurangan dari algoritma *El-Gamal* dan Steganografi, akan lebih baik digabungkan keduanya untuk mengamankan data sehingga tingkat kerahasiaan dan keamanan data menjadi lebih baik.

Berdasarkan latar belakang yang telah diuraikan diatas, maka penulis membuat "**Aplikasi Pembelajaran Kriptografi Menggunakan Algoritma *El-Gamal* dan Steganografi Berbasis Desktop".**

1.2 Identifikasi Masalah

Identifikasi masalah berdasarkan latar belakang di atas adalah sebagai berikut:

1. Media pembelajaran untuk mempelajari kriptografi khususnya dengan algoritma *El-Gamal* masih sangat kurang.
2. Membuktikan penerapan implementasi algoritma kriptografi *El-Gamal* untuk mengenkripsi data berupa teks, dengan teknik steganografi untuk disisipkan ke dalam gambar.

1.3 Tujuan Penelitian

1. Aplikasi ini menjadi media pembelajaran kriptografi untuk keamanan data teks menggunakan algoritma *El-Gamal*.
2. Aplikasi ini menggunakan algoritma *El-Gamal* untuk memproteksi data teks, dan teknik steganografi untuk penyisipan teks yang telah dienkripsi ke dalam gambar.

1.4 Batasan Masalah

Berdasarkan dari apa yang telah dipaparkan diatas, maka batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Teknik pengamanan data teks menggunakan algoritma kriptografi El-Gamal dan untuk penyisipannya dengan teknik steganografi.
2. Data yang akan dienkripsi maupun didekripsi berbentuk file. File tersebut berupa teks (.txt), dan untuk penyisipan gambarnya berekstensi (.bmp).
3. Bilangan Prima p lebih besar dari 255.
4. Implementasi algoritma ini dibangun dengan bahasa pemrograman C# dan Microsoft Visual Studio 2012.

5. Teks yang akan dienkripsi tidak lebih dari 200 karakter.

1.5 Manfaat Penelitian

Melalui penelitian ini diharapkan dapat memperoleh manfaat sebagai berikut:

1. Peneliti bisa mengetahui cara mengamankan data dengan metode pengenkripsian data dan penyisipan ke dalam gambar dengan teknik steganografi.
2. Dapat mengimplementasikan kriptografi menjadi aplikasi yang dapat digunakan perusahaan atau instansi yang memperhatikan kerahasian data penting perusahaannya apabila aplikasi ini dikembangkan lagi.
3. Dengan implementasi ini diharapkan pesan rahasia dapat disimpan dengan sebaik mungkin dengan memanfaatkan algoritma *El-Gamal* dan menjadi referensi untuk penelitian selanjutnya di bidang kriptografi.
4. Dapat menjadi media pembelajaran untuk mahasiswa maupun dalam bidang keamanan data khususnya mata kuliah kriptologi dan proteksi data.

1.6 Sistematika Penulisan

Penulis mencoba memberikan sedikit gambaran tentang isi laporan ini secara sistematis yang tersusun sebagai berikut:

1. BAB I PENDAHULUAN

   Dalam bab ini berisikan tentang latar belakang penelitian, identifikasi masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan sistematika penulisan laporan.

2. BAB II STUDI PUSTAKA

   Dalam bab ini berisi kajian keislaman yang berkaitan dengan penelitian, kajian teori, konsep perancangan, bahasa pemrograman dan alat yang digunakan, konsep pengujian, dan beberapa kajian terdahulu yang mendukung dalam pembangunan aplikasi.

3. BAB III METODOLOGI PENELITIAN

   Dalam bab ini berisi tentang metode penelitian yang dilakukan, yaitu metode algoritma *El-Gamal*, tahapan dalam melakukan penelitian, perangkat penelitian, waktu dan perencanaan penelitian.

4. BAB IV ANALISIS DAN PERANCANGAN

   Berisi tentang analisis sistem yang meliputi analisis sistem berjalan, analisis permasalahan, analisis solusi, kebutuhan sistem dan perancangan sistem yang berisi perancangan sistem yang diusulkan.

5. BAB V IMPLEMENTASI DAN PENGUJIAN

   Berisi implementasi dan pengujian bertahap dari aplikasi yang dibuat.

6. BAB VI KESIMPULAN DAN SARAN

   Berisi kesimpulan dari uraian pada bab sebelumnya dan saran untuk pengembangan aplikasi yang dirancang.