BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan dan perkembangan teknologi informasi sudah menjadi sangat pesat dan berpengaruh dalam kehidupan manusia, tak terkecuali dalam hal pertukaran data. Pada dasarnya, pertukaran data dilakukan tanpa melakukan pengamanan pada data yang dikirim. Seiring dengan perkembangan, maka proses pertukaran data dituntut memiliki sistem kemanan yang diharapkan mampu untuk menjaga integritas data dari pihak-pihak yang memanfaatkan celah dengan mengambil data, merusak, maupun mengubah data untuk kemudian dijadikan sebagai kepentingan pribadi atau kelompok (Pavese & Forbes, 2009).

Untuk menutup celah tersebut, maka salah satu cara yang dapat digunakan untuk mengamankan data adalah dengan menyandikan data menjadi kode-kode yang tidak dimengerti oleh pihak-pihak yang tidak berhak dan hanya dimengerti oleh pihak-pihak terkait. Namun yang menjadi perhatian adalah, apakah data yang dikirim sudah sepenuhnya aman dari serangan? Kemajuan, peningkatan, dan perkembangan sejatinya adalah hal yang positif. Akan tetapi tidak selamanya hal positif yang akan muncul, karena seiring dengan itu akan muncul pula sisi negatifnya (Renninger, 1974). Inilah yang menjadi latar belakang berkembangnya sistem keamanan untuk melindungi data.

Namun, untuk membangun sebuah sistem tentulah diperlukan beberapa metode atau teknik. Banyak sekali metode atau teknik yang sekarang digunakan untuk melakukan penyandian. Metode atau teknik ini biasa dikenal sebagai

Kriptografi. Pada awal perkembangannya, teknik kriptografi yang digunakan adalah kriptografi simetri. Kriptografi simetri adalah teknik kriptografi yang hanya menggunakan satu kunci untuk melakukan proses enkripsi dan dekripsi. Selanjutnya teknik kriptografi dikembangkan menjadi kriptografi asimetri, yaitu teknik kriptografi yang menggunakan dua kunci berbeda masing-masing untuk proses enkripsi dan dekripsi (Ariyus, 2008).

ElGamal adalah salah satu algoritma yang termasuk dalam kategori kriptografi asimateri. ElGamal adalah algoritma kriptografi yang ditemukan oleh ilmuwan Mesir, yaitu Taher ElGamal pada tahun 1985. Algoritma ElGamal mendasarkan kekuatannya pada fakta matematis sulitnya menghitung logaritma diskrit (Rochmat dkk, 2012).

Pada mulanya algoritma ini digunakan untuk kepentingan *digital signature*, namun kemudian dimodifikasi sehingga dapat digunakan untuk enkripsi dan dekripsi. Algoritma ElGamal pernah dipercaya sebagai metode penyandian, seperti aplikasi PGP dan GnuPG yang dapat digunakan untuk pengamanan *e-mail* dan tanda tangan digital (Zelvina dkk, 2012). Pada tahun 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard*, sebuah mekanisme penyandian yang berdasar pada algoritma ElGamal (Menezes dkk, 1997).

Salah satu kelemahan yang masih menjadi sorotan dalam kriptografi adalah faktor *size* (beban data). Karena semakin tinggi tingkat keamanan suatu algoritma kriptografi, biasanya disertai dengan meningkatnya beban data pada proses enkripsi dan dekripsinya (William, 2009). Hal ini dibuktikan oleh algoritma ElGamal yang memiliki panjang *ciphertext* (data terenkripsi) dua kali panjang *plaintext* (data awal) (Caroline, 2011). Oleh karena itu, diperlukan sebuah proses

untuk mereduksi jumlah beban data yang dihasilkan oleh algoritma ElGamal ini. Proses yang mengonversikan sebuah data menjadi sebuah data lain dengan ukuran data yang lebih kecil. Metode atau teknik ini disebut Kompresi (Salomon & Motta, 2010).

Lempel-Ziv-Welch atau yang biasa disebut LZW ini adalah satu dari banyak algoritma kompresi. LZW merupakan algoritma yang dikembangkan oleh Terry Welch pada tahun 1984 dari algoritma LZ78, algoritma kompresi yang dibuat oleh Abraham Lempel dan Jakob Ziv pada tahun 1978. LZW sama dengan algoritma kompresi berbasis kamus lainnya seperti Huffman, dimana urutan nilai dalam aliran data yang mengulang lebih dari sekali dieksploitasi untuk mengompres data (Terras, 2008). Metode LZW telah digunakan pada sistem operasi UNIX dan LINUX, dan juga pada aplikasi *compress*, *uncompress*, *gzip*, dan *gunzip*. LZW menjadi teknik untuk kompresi data dalam komputer pengolah kata. Algoritma kompresi ini digunakan dalam ARC dan menjadi basis kompresi citra dalam format file GIF (Putra, 2010).

Dengan berpedoman pada paparan diatas, maka akan dibangun sebuah aplikasi untuk mengamankan dokumen digital dengan mengimplementasikan algoritma kriptografi ElGamal dan algoritma kompresi LZW.

1.2. Perumusan Masalah

Masalah yang dirumuskan dalam penelitian ini adalah “Bagaimana mengimplementasikan algoritma kriptografi ElGamal ke dalam sebuah aplikasi sehingga mampu untuk mengamankan dokumen digital?”. Selain itu, “Bagaimana

mengimplementasikan algoritma kompresi LZW untuk mengompresi dokumen hasil enkripsi sehingga ukurannya dapat dikurangi?".

1.3. Batasan Masalah

Penelitian akan berpusat pada implementasi algoritma ElGamal ke dalam sebuah aplikasi sehingga mampu untuk mengamankan dokumen digital, kemudian memanfaatkan algoritma LZW untuk memperkecil ukuran dokumen hasil enkripsi tersebut. Adapun pembatasan masalah lainnya dalam penelitian ini adalah sebagai berikut.

a. Aplikasi ini dibuat hanya sebagai Windows *desktop application*.
b. Dokumen-dokumen digital yang dapat digunakan dalam aplikasi ini (*input*) hanya yang ber-ekstensi (.txt), (.pdf), (.doc), (.docx), (.xls), (.xlsx), (.ppt), dan (.pptx).

1.4. Tujuan Penelitian

Penelitian bertujuan untuk mengimplementasikan algoritma kriptografi ElGamal dan kompresi LZW pada sebuah aplikasi sehingga mampu untuk mengamankan dokumen digital dengan beban data hasil keluaran (output) yang lebih ringan.

1.5. Manfaat Penelitian

Secara umum, dengan dibangunnya aplikasi ini, maka para pengguna diharapkan dapat menggunakannya untuk mengamankan dokumen-dokumen

digital mereka. Secara khusus untuk mengamankan dokumen-dokumen yang dianggap penting dan bersifat rahasia.

Dengan pengaplikasian algoritma kriptografi ElGamal dan kompresi LZW ini diharapkan dapat memenuhi kebutuhan dunia akan adanya aplikasi yang dapat digunakan untuk mengamankan dokumen dengan beban data hasil keluaran (*output*) yang lebih ringan.

1.6. Sistematika Penulisan

Laporan ini tersusun menjadi beberapa bab dengan penjelasan masing-masing bab adalah sebagai berikut.

Bab I: Pendahuluan

Bab ini berisikan tentang latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan laporan.

Bab II: Landasan Teori

Bab ini berisikan teori-teori terkait dengan pelaksanaan penelitian ini. Teori-teori yang digunakan antara lain adalah teori mengenai kriptografi, kompresi, dan teori pendukung lainnya. Secara khusus teori mengenai algoritma kriptografi ElGamal dan algoritma kompresi LZW.

Bab III: Analisis dan Perancangan

Bab ini berisikan metode penelitian, analisis penulis mengenai penerapan algoritma ElGamal dan LZW pada aplikasi, perancangan

aplikasi dan pengimplementasiannya, disertai dengan berbagai diagram sebagai pendukung.

Bab IV: Implementasi dan Uji Coba

Bab ini berisikan hasil pengimplementasian rancangan dan uji coba terhadap hasil implementasi beserta dengan analisis dan pembahasan dari hasil yang diperoleh tersebut.

Bab V: Kesimpulan dan Saran

Bab ini berisikan kesimpulan penulis mengenai aplikasi yang telah dibangun secara keseluruhan, serta beberapa saran yang dapat diterapkan untuk pengembangan aplikasi di waktu mendatang.