BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan dan perkembangan teknologi saat ini telah mempengaruhi segala aspek kehidupan, termasuk aspek penyimpanan data, sepeti dalam penyimpanan data pada *file* dokumen saat ini sering digunakan oleh banyak pihak. Keamanan dan kerahasiaan merupakan aspek yang sangat penting dalam proses penyimpanan data pada *file* dokumen. Untuk menjaga keamanan dan kerahasiaan suatu *file* terutama bagi perusahaan, instansi, atau organisasi-organisasi yang mempunyai dokumen-dokumen penting tersebut agar terhindar dari gangguan pihak luar. Saat ini, sebagian besar dokumen-dokumen seperti *Microsoft Office* telah mempunyai suatu sitem pengamanan tersendiri, namun sistem pengamanan tersebut masih terbilang mudah untuk diketahui oleh pihak lain.

Dengan semakin meningkatnya penggunaan aplikasi seperti *Microsoft Office* ini maka kita butuhkan pula cara untuk meningkatkan keamanan pada data terhadap dokumen tersebut. Hal ini dikarenakan setiap perusahaan atau instansi sangat mungkin memiliki suatu data yang tidak boleh semua orang mengetahuinya. Banyak usaha yang dilakukan suatu perusahaan untuk

mengamankan data dari ancaman pihak luar yang tidak memiliki hak untuk mengolah atau merusak data dokumen tersebut.

Salah satu cara yang bisa digunakan untuk mempertahankan kerahasiaan dari data tersebut adalah dengan tehnik penyandian. Dengan mennggunakan cara ini, maka setiap data asli (*plainteks*) akan disandikan terlebih dahulu sedemikian sehingga menjadi kode-kode yang tidak bisa dipahami maksudnya (*cipherteks*), sehingga bila ada pihak luar yang ingin mengetahui atupun bermaksud merubahnya akan kesulitan dalam menerjemakan isi data yang sebenarnya, teknik tersebut dikenal dengan teknik *kriptografi.*

Dalam penelitian kali ini algoritma yang akan digunakan dalam proses enkripsi dan dekripsi adalah Algoritma ElGamal, dimana algoritma ini termasuk algoritma asimetris atau penggunaan dua kunci dalam proses enkripsi dan deskripsinya. Keunggulan algoritma Elgamal sulitnya menghitung logaritma diskrit pada bilangan modulo prima yang besar.

Pembuatan aplikasi pastilah menggunakan suatu bahasa pemrograman tertentu, sedangkan bahasa pemrograman yang dipakai untuk pembuatan aplikasi berbasis web kali ini adalah bahasa program HTML dan Javasricpt. Dari penjabaran yang telah dijelaskan penulis di atas, maka dari itu penulis akan membuat suatu judul yaitu, “Aplikasi pengamanan dokumen menggunakan algoritma kunci publik Elgamal”.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, dapat dirumuskan masalah yang ada untuk pembahasan skripsi, yaitu : “Bagaimana aplikasi pengamanan dokumen menggunakan kunci publik elgamal?”

1.3 Batasan Masalah

Setiap penelitian mempunyai ruang lingkup danbatasan masalah, dalam penelitian ini batasan masalah yang ada yaitu sebagai berikut :

1) Format yang akan dienkripsi antara lain file .doc, .xls, .ppt, .pdf, dan .jpeg.
2) Algoritma yang digunakan untuk enkripsi dan dekripsi adalah algoritma Elgamal.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah untuk mengamankan dan menjaga kerahasiaan suatu *file* dokumen agar terhindar dari penyalahgunaan dan pengubahan data dari oknum-oknum yang tidak bertanggung jawab.

1.4.2 Manfaat Penelitian

Manfaat yang terdapat didalam penelitian adalah suatu yang wajib sekali untuk dibahas, kali ini manfaat akan dibagi menjadi 3 sisi yaitu bagi penulis, pembaca dan *user* (pengguna). Seperti berikut ini :

1) Bagi Penulis :

   Memperdalam ilmu pengetahuan tentang penggunaan algoritma Elgamal untuk enkripsi dan dekripsi file pada suatu dokumen dan mengetahui bagaimana cara mengembangkan ilmu yang diperoleh selama perkuliahan serta mengetahui sejauh mana penguasaan materi yang sudah didapat.

2) Bagi Pengguna Aplikasi (*user*):

   File yang dikelola pada suatu dokumen aman dari oknum yang tidak bertanggung jawab dan juga untuk menjaga kerahasiaan tersendiri dari dokumen tersebut.

3) Bagi Pembaca:

   Dapat mengetahui, memahami dan mempelajari konsep dari algoritma Elgamal untuk enkripsi dan dekripsi data serta diharapkan bisa menjadi bahan referensi penelitian dibidang kriptografi.

1.5 Waktu dan Tempat

1.5.1 Waktu Penelitian

Penelitian ini dilakukan pada semester genap Tahun Akademik 2018/2019, yaitu antara bulan September 2019 sampai bulan Oktober 2019.

1.5.2 Tempat Penelitian

Penelitian ini dilakukan di daerah Plaju, Sebrang Ulu I kota Palembang pada Universitas Bina Darma.

1.6 Metodelogi

1.6.1 Metode Penelitian

Menurut Darmadi (2013:153) metode penelitian adalah suatu cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Metode yang digunakan pada penelitian ini adalah metode eksperimen. Jaedun (2011:03) menyatakan bahwa penelitian eksperimen pada umumnya digunakan dalam penelitian yang bersifat laboratoris, juga merupakan satu-satunya metode penelitian yang dianggap paling dapat menguji hipotesis hubungan sebab-akibat atau paling dapat memenuhi validitas internal.

1.6.2 Metode Pengembangan Perangkat Lunak

Tahapan pengembangan sistem dalam perancangan aplikasi pengamanan dokumen berbasis *web* ini dengan menggunakan metodologi *Rational Unified Process*. *Rational Unified Process* (RUP) adalah pendekatan pengembangan perangkat lunak yang dilakukan berulang-ulang (*iterative*), fokus pada arsitektur (*architecturecentric*), lebih diarahkan berdasarkan penggunaan kasus (Aunur R. Mulyanto, 2008) Dengan menggunakan model ini, RUP membagi tahapan pengembangan perangkat lunaknya ke dalam 4 fase sebagai berikut:

1. *Inception*

   Pada tahap ini penulis mendefinisikan batasan kegiatan, melakukan analisis kebutuhan pengguna, melakukan perancangan awal perangkat lunak, pemodelan diagram UML (*use case diagram*), dan pembuatan dokumentasi.

2. *Elaboration*

   Tahap untuk melakukan desain secara lengkap berdasarkan hasil analisis ditahap *inception.* Aktivitas yang dilakukan pada tahap ini antara lain mencakup pembuatan desain arsitektur subsistem (*architecture pattern*), desain komponen sistem, desain format data (protokol komunikasi), desain antarmuka/tampilan, desain peta aliran tampilan, penentuan *design pattern* yang digunakan, pemodelan diagram UML (diagram *activity, class*) dan pembuatan dokumentasi.

3. *Construction*

   Tahap untuk mengimplementasikan hasil dan melakukan pengujian hasil implementasi. Pada tahap awal *construction,* dilakukan pemeriksaan ulang hasil analisis dan desain, apabila desain yang dibuat telah sesuai dengan analisis sistem, maka implementasi dengan bahasa pemrograman java dapat dilakukan. Aktivitas yang dilakukan tahap ini antara lain mencakup pengujian hasil analisis dan desain, pendataan kebutuhan implementasi lengkap (berpedoman pada identifikasi kebutuhan di tahap analisis), penentuan *codding pattern* yang digunakan, pembuatan program, pengujian,optimasi,program,pendataan berbagai kemungkinan pengemban gan/perbaikan lebih lanjut, dan pembuatan dokumentasi.

4. *Transition*

   Tahap untuk menyerahkan sistem ke konsumen (roll-out), yang umumnya mencakup pelaksanaan pelatihan kepada pengguna dan testing beta aplikasi terhadap ekspetasi pengguna.

1.6.3 Alat Penelitian

Dalam penelitian ini penulis menggunakan alat penelitian berupa perangkat keras dan perangkat lunak dengan spesifikasi minimum yang diperlukan dalam pembuatan aplikasi adalah sebagai berikut :

1. **Perangkat Keras**

Perangkat keras yang digunakan yaitu Laptop Acer dengan *memory* 4 GB, *Harddisk* 1TB, *keyboard, mouse, printer, dan scanner*.

2. **Perangkat lunak**

Perangkat lunak yang digunakan berupa Sistem Operasi Windows 10, Ms. Office, paket web server (Apache 5.6.23, PHP, MySQL), HTML dan Javascript sebagai text editor.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini dimaksudkan agar dapat menjadi pedoman atau garis besar penulisan laporan penelitian ini dan dapat menggambarkan secara jelas isi dari laporan penelitian sehingga terlihat hubungan antara bab awal hingga bab terakhir. Sistem penulisan laporan penelitian ini terdiri atas:

BAB I : PENDAHULUAN

Pada bab ini dibahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian yang digunakan, metode analisis data, metode pengujian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Bab II ini berisi landasan teori, yaitu teori–teori umum dan khusus yang mendukung penulisan skripsi ini. Hal-hal yang tercakup di dalamnya adalah pembahasan tentang Aplikasi, Algoritma Elgamal, HTML, Javascript.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini membahas tentang analisis, perancangan dan pembuatan Aplikasi pemgamanan dokumen menggunakan algoritma kunci publik Elgamal.

BAB IV : HASIL DAN PEMBAHASAN

Bab ini berisi hasil dan pembahasan mengenai Aplikasi pengamanan dokumen menggunakan algoritma kunci publik Elgamal yang dihasilkan oleh penelitian ini.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan-kesimpulan yang didapat dari hasil penelitian dan saran-saran untuk perbaikan/pengembangan selanjutnya dari hasil penelitian ini.