

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

LKP Bhaskoro *Training Education Centre* adalah sebuah lembaga pendidikan yang mengkhususkan diri dalam pendidikan bahasa Jepang dan pengiriman peserta magang ke Jepang. LKP Bhaskoro sebagai pengirim peserta magang dan rekanan perusahaan di Jepang sebagai penerima peserta magang saling bertukar dokumen rahasia. Dokumen ini tidak boleh diketahui orang lain. Kebocoran dokumen mengakibatkan hilangnya kepercayaan rekanan perusahaan di Jepang terhadap LKP Bhaskoro *Training Education Centre*, sehingga mengakibatkan terhentinya pengiriman peserta magang ke Jepang. Berdasarkan hal tersebut, maka diperlukan sebuah aplikasi keamanan dokumen. Aplikasi keamanan dokumen yang dibutuhkan adalah sebuah aplikasi yang mampu menyembunyikan informasi yang terdapat dalam dokumen tersebut. Aplikasi tersebut juga harus mampu mengembalikan informasi yang terdapat dalam dokumen ke bentuk aslinya.

Metode yang dipilih untuk menyelesaikan permasalahan tersebut di atas adalah dengan melakukan enkripsi pada dokumen tersebut menggunakan algoritma kriptografi Elgamal. Algoritma ini dipilih karena termasuk dalam kategori algoritma asimetris yang berarti bahwa kunci untuk enkripsi dan kunci untuk dekripsi berbeda. Kunci untuk enkripsi disebut kunci *public* bisa diberikan kepada rekanan perusahaan di Jepang. Kunci untuk dekripsi disebut kunci *private* harus disimpan, tidak boleh diketahui oleh pihak lain.

Implementasi keamanan dokumen dibuat menggunakan teknologi java, karena java dapat dijalankan di semua platform. Java bersifat *neutral architecture* karena program Java dirancang untuk menghasilkan kode yang netral terhadap semua arsitektur perangkat keras.

1.2. Perumusan Masalah

Berdasarkan latar belakang masalah di atas penulis merumuskan masalah yaitu “Bagaimana membuat aplikasi keamanan dokumen yang siap diterapkan di LKP Bhaskoro *Training Education Centre* menggunakan algoritma kriptografi Elgamal dengan bahasa pemrograman java berbasis desktop”.

1.3. Pembatasan Masalah

Agar tidak terlepas dari maksud pembuatan skripsi maka peneliti membatasi permasalahan pada:

1. Masalah yang dibahas adalah kriptografi Elgamal untuk dokumen yang berekstensi *doc*, *docx*, *xls* dan *xlsx*.
2. Data dokumen yang diambil adalah dokumen di LPK Bhaskoro Sukoharjo.
3. Input data adalah sesuai dengan data dokumen pada LPK Bhaskoro Sukoharjo.
4. Output data adalah dokumen yang telah di enkripsi (*ciphertext*).
5. Bahasa pemrograman yang digunakan adalah java yang dibangun dengan aplikasi Netbeans.

1.4. Tujuan Skripsi

Tujuan yang ingin dicapai dalam penyusunan skripsi yang berjudul “Aplikasi Keamanan Dokumen pada LKP Bhaskoro Training Education Centre menggunakan Algoritma Kriptografi Elgamal dengan Bahasa Pemrograman Java Berbasis Desktop” yaitu terbentuknya aplikasi keamanan dokumen menggunakan algoritma kriptografi Elgamal dengan bahasa pemrograman java berbasis desktop yang siap diterapkan di LKP Bhaskoro *Training Education Centre*.

1.5. Manfaat Skripsi

Penyusunan skripsi ini diharapkan dapat memberikan manfaat bagi:

1.5.1. Bagi Akademik

Dapat dijadikan sebagai pustaka dan referensi bagi mahasiswa lain yang melakukan penelitian dengan topik yang berhubungan.

1.5.2. Bagi Penulis

Dapat menerapkan ilmu pengetahuan yang diperoleh selama kuliah dan untuk menambah pengetahuan khususnya disiplin ilmu yang diteliti.

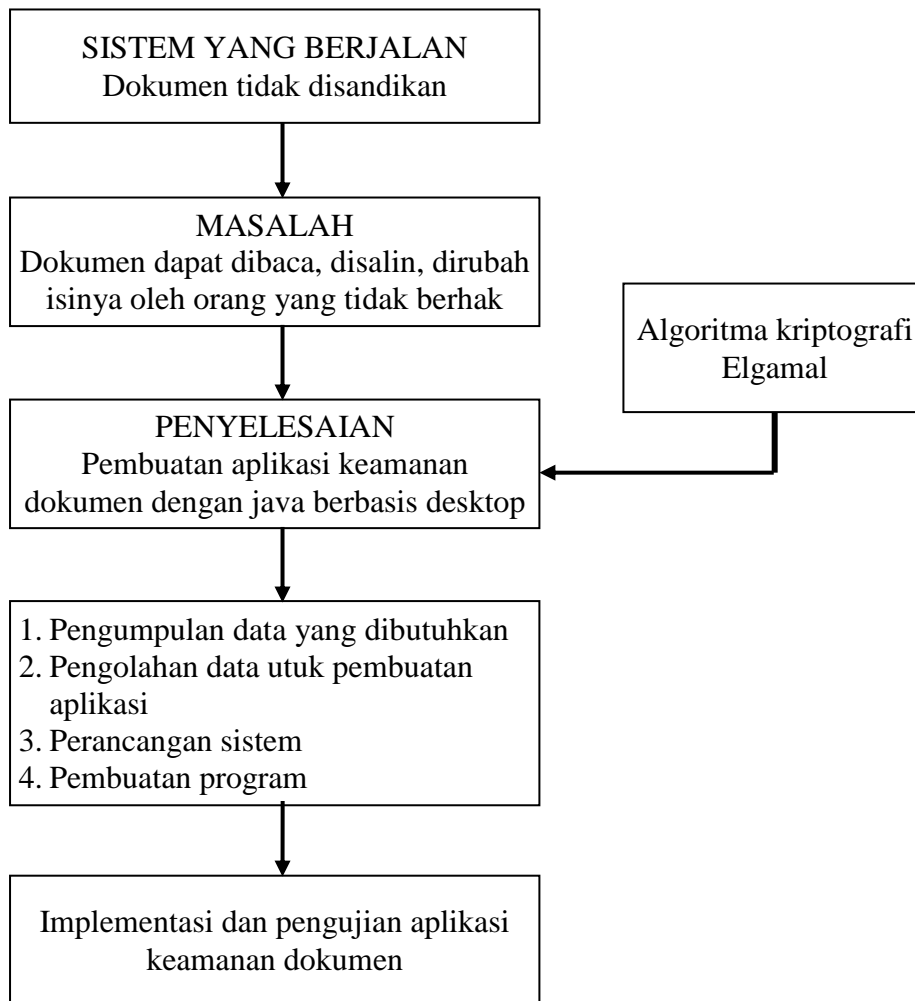
1.5.3. Bagi Instansi

Mampu memberikan solusi terhadap permasalahan keamanan dokumen di LKP Bhaskoro *Training Education Centre*.

1.6. Kerangka Pikir

Kerangka pikir berguna untuk memberikan penjelasan mengenai hal-hal apa saja yang melandasi penelitian, sistematika pembuatan serta hasil akhir yang ingin dicapai dalam penelitian.

Berikut adalah skema kerangka pikir penelitian:



Gambar 1. 1 Skema Pemikiran Penelitian

1.7. Sistematika Penulisan

BAB I : Pendahuluan

Pendahuluan berisi tentang Latar Belakang Masalah, Perumusan Masalah, Pembatasan Masalah, Tujuan Skripsi, Manfaat Skripsi, Kerangka Pikir, Sistematika Penulisan.

BAB II : Landasan Teori

Landasan Teori berisi uraian sistematis mengenai teori-teori dan hasil penelitian yang relevan dengan variabel-variabel yang diteliti. Dalam landasan teori diberikan penjelasan mengenai variabel-variabel yang diteliti, melalui pendefinisian yang lengkap dan mendalam. Selain itu juga menjelaskan tentang teori-teori yang dipakai untuk menyelesaikan masalah.

BAB III : Metode Penelitian

Metode Penelitian berisi tentang uraian metode-metode yang digunakan penulis dalam melakukan penelitiannya, meliputi jenis dan sumber data, teknik pengumpulan data, alat penelitian dan tahap penelitian.

BAB IV : Tinjauan Umum Obyek Penelitian

Tinjauan Umum Obyek Penelitian menguraikan tentang gambaran umum mengenai objek yang diteliti, meliputi variabel yang digunakan dalam algoritma Elgamal, pembangkitan kunci, perhitungan manual enkripsi dan dekripsi dalam algoritma Elgamal.

BAB V : Pembahasan

Pembahasan berisi tentang pembuatan aplikasi keamanan dokumen, meliputi pembuatan *flowchart* dan algoritma aplikasi keamanan dokumen, *flowchart* dan algoritma pembangkitan kunci, *flowchart* dan algoritma proses enkripsi, *flowchart* dan algoritma proses dekripsi, perancangan antar muka (*interface*),

implementasi algoritma Elgamal dalam bahasa pemrograman java, dan hasil pengujian aplikasi.

BAB VI : Penutup

Penutup berisi tentang kesimpulan dari masalah yang diteliti dan saran yang berupa anjuran atau rekomendasi yang perlu dilakukan untuk membawa penelitian ke tahap berikutnya.

Lampiran : Daftar Pustaka

Daftar Pustaka berisi tentang sumber informasi yang digunakan dalam penyusunan laporan skripsi

Lampiran-lampiran

Berisi tentang informasi atau materi lainnya yang belum disampaikan pada bab-bab sebelumnya