BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin suatu informasi mudah didapat dan digunakan maka teknologinya pun akan semakin canggih. Akibat semakin canggih sistem yang digunakan maka tidak lepas dari berbagai macam resiko. Kehandalan sistem dalam berbagi pakai dan kemudahan dalam penyajian informasi tidak dapat dihindari. Termasuk penyajian informasi yang bersifat pribadi, rahasia, internal dan sebagainya.

Salah satu sistem yang paling rentan terhadap pencurian informasi adalah teknologi *smart card* yaitu media pertukaran data pada sistem berbasis kartu. Teknologi *smart card* bukanlah hal yang baru, penggunaan *smart card* sudah umum kita jumpai seperti pada kartu kredit, bidang pendidikan seperti kartu siswa/mahasiswa, perhubungan, industri jasa hingga digunakan sebagai kartu identitas multifungsi seorang karyawan pada suatu perusahaan. Oleh karena itu, dibutuhkan keamanan data yang handal ketika terjadinya pertukaran data dalam sistem.

Pembobolan rekening bank menghiasi berita baru-baru ini. Selain dengan cara penipuan undian lewat sms, transaksi kartu kredit, *ATM Skimming* juga perlu diwaspadai. Istilah ini digunakan untuk kejahatan dengan modus pencurian data melalui kartu ATM atau kartu kredit nasabah bank.

Lalu bagaimana solusi agar sistem mampu menangani pembatasan akses terhadap informasi yang bersifat pribadi. Dari itu, maka dibuatlah suatu teknik penyandian yang disebut kriptografi untuk mengamankan data yang bersifat *private*.

Dalam pengiriman berkas dapat dimanipulasi isinya oleh pihak ketiga sehingga pesan dengan makna yang berbeda akan diterima penerima dan tujuan pengiriman tidak tercapai. Oleh karena itu, dibutuhkan sebuah mekanisme untuk menjamin bahwa pesan yang diterima penerima, berisi informasi yang dikirimkan oleh pengirim.

Namun masalah lain muncul ketika data hasil penyandian (kriptografi) digandakan (*chosen-chipertext attack*). Seorang pembajak (*hacker*) tidak perlu mengembalikan data ke dalam plainteks, dia cukup menggandakan data hasil penyandian dari *smart card*. Lalu bagaimana jaminan keamanan dari kriptografi.

Berdasarkan hal tersebut, maka dilakukan analisis kriptografi atau teknik penyandian yang dapat membantu mengamankan data juga menjamin informasi yang diterima sesuai dengan informasi yang dikirimkan termasuk pengecekan legalitas ketika suatu data pada *smart card* berhasil digandakan.

1.2 Identifikasi Masalah

Dari uraian latar belakang diatas, maka hal yang dapat diidentifikasi adalah bagaimana mengatasi masalah keamanan data pada sistem berbasis *smart card* menggunakan kriptografi *ElGamal* dan penanganan *chosen-chipertext attack* menggunakan algoritma *Luhn*.

1.3 Maksud dan Tujuan

3.1 Maksud

Maksud dari penelitian ini adalah membuat sistem penyandian data dengan teknik kriptografi ElGamal dan algoritma Luhn yang digunakan untuk pencegahan penggandaan informasi pada *smart card.*

3.2 Tujuan

Adapun tujuan yang ingin dicapai setelah analisis dan implementasi penelitian ini adalah :

1. Mengamankan data yang tersimpan pada *smart card.*
2. Memberikan solusi penanganan *chosen-chipertext attack* pada *smart card*.

1.4 Batasan Masalah

Tentunya ruang lingkup yang dibahas akan sangat luas dan banyak sekali masalah yang akan muncul. Namun penulis membatasi permasalahanya sebagai berikut :

1. Algoritma penyandian yang digunakan adalah algoritma ElGamal.
2. Algoritma validasi menggunakan Luhn.
3. *Smart card* yang digunakan sebagai media implementasi (*read/write)* adalah tipe sistem operasi (ACOS).
4. Data yang akan disandikan/dienkripsi adalah data yang terlibat dalam validasi, diantaranya NIM, No Rekening, PIN, CSPRNG RSA dan LUHN.
5. Implementasi dari hasil analisis diterapkan pada suatu program agar mempermudah pemahaman dengan fungsional yang disesuaikan.

6. Program yang dibuat tidak menggunakan database dan merupakan fase dimana data pada kartu pertama kali dibuat.

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan menggunakan metode analisis deskriptif yaitu suatu metode yang bertujuan untuk mendapatkan gambaran yang jelas tentang hal-hal yang diperlukan, melalui tahapan sebagai berikut :

1.5.1 Pengumpulan Data

Pada tahap ini prosedur yang dilakukan adalah mencari sebanyak mungkin data dari berbagai sumber seperti internet, buku, jurnal, artikel blog, catatan kuliah perusahaan yang akan dijadikan sebagai informasi sebagai landasan teori. Diantaranya informasi yang berhubungan dengan permasalahan yang akan dibahas yang dapat membantu dalam menganalisis logaritma diskrit dan algoritma cek digit suatu angka berdasarkan digit-digit yang membentuknya.

1.5.2 Pengembangan Perangkat Lunak

Model yang digunakan dalam pembuatan perangkat lunak adalah model *Waterfall*, yang terdiri dari beberapa proses, yaitu :

1. Definisi kebutuhan

   Menetapkan elemen-elemen yang dibutuhkan dalam pembuatan perangkat lunak.

2. Analisis dan perancangan

   Analisis terhadap perangkat lunak yang akan dibangun dan menentukan arsitektur tampilan akan digunakan pada program dengan fungsional yang disesuaikan.

3. Kode

   Tahap penerjemahan data atau pemecahan masalah yang telah dirancang kedalam bahasa pemrograman tertentu.

4. Pengujian

   Dilakukan pada perangkat lunak yang dibangun. Apakah telah sesuai dengan hasil yang diharapkan.

1.6 Sistematika Penulisan

Agar mencapai hasil yang baik dan terarah serta tidak menyimpang dari permasalahan yang ada maka dibuatlah sistematika penelitian yang diuraikan sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang, perumusan masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori pendukung dalam menganalisis logaritma diskrit yang digunakan oleh elgamal dalam melakukan penyandian, algoritma cek digit yang digunakan untuk mengecek validitas suatu angka berdasarkan digit-digit yang membentuknya serta wawasan-wawasan mengenai kriptografi dan contoh pemanfaatanya pada *smart card*.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan analisis terhadap seluruh spesifikasi aplikasi yang akan dibangun baik dilihat dari kekurangan dan kelebihannya. Juga perancangan program yang dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini membahas bagaimana pengimplementasian dan pengujian terhadap program. Untuk melihat apakah sistem yang dibangun sudah sesuai dengan hasil yang diharapkan atau belum.

BAB V KESIMPULAN DAN SARAN

Pada bab ini membahas tentang kesimpulan dari hasil pembahasan serta saran–saran tentang implementasi dari kriptografi elgamal dan algoritma luhn pada program serderhana.