BAB I

PENDAHULUAN

Pada Bab I akan dijelaskan mengenai beberapa hal, yaitu latar belakang masalah, identifikasi masalah, rumusan masalah, tujuan, pembatasan masalah, metodologi penelitian, spesifikasi alat dan sistematika penulisan yang berkaitan dengan Laporan Tugas Akhir ini.

1.1 Latar Belakang Masalah

Penggunaan perangkat komputer pada abad ke – 21 oleh umat manusia semakin berkembang pesat. Berbagai macam aktivitas yang dilakukan manusia semakin membutuhkan hal tersebut.[1] Salah satu alat yang mendukung penggunaan perangkat komputer adalah *smart card*. Alat ini berwujud sebuah kartu dengan ukuran seperti kartu kredit. Di dalam kartu tersebut, terdapat sebuah bagian yang disebut *chip* yang berfungsi untuk menyimpan informasi mengenai data pribadi seseorang. Data pribadi tersebut diperlukan untuk mengidentifikasi dan mengotentifikasi pengguna saat mengakses berbagai fasilitas di dalam wilayah penggunaan dari *smart card*.

Untuk mendukung penggunaan *smart card* tersebut, digunakan sebuah alat bantu identifikasi *chip* yang disebut sebagai *reader*. Alat ini dapat berkomunikasi dengan *smart card* melalui bantuan gelombang frekuensi radio (RFID / *Radio Frequency Identification*) untuk mengaktifkan bagian *chip* pada *smart card* sehingga dapat mengirimkan informasi di dalamnya ke perangkat *reader*.[1] Informasi yang telah didapatkan oleh perangkat *reader* lalu diproses menggunakan aplikasi perangkat lunak tertentu untuk membaca atau mengubah isi dari informasi di dalam *smart card* tersebut.

Dalam penggunaannya sehari – hari, data di dalam *smart card* dapat dicuri dan disalahgunakan oleh orang – orang yang tidak bertanggungjawab sehingga merugikan pengguna *smart card*. Oleh karena itu metode

perlindungan data perlu diterapkan untuk meningkatkan keamanan suatu data. Salah satu metode itu disebut sebagai kriptografi. Proses kriptografi bekerja dengan cara memanipulasi suatu data asli sehingga menghasilkan keluaran data yang akan teracak. Proses kriptografi sendiri terdiri dari dua tahap, yaitu proses enkripsi yang bertujuan untuk mengacak data asli (*plaintext*) dengan bantuan variabel pengacak yang disebut sebagai *key* sehingga tidak dimengerti menggunakan bahasa manusia, serta proses dekripsi yang bertujuan untuk mengembalikan data yang telah teracak (*ciphertext*) sehingga menjadi *plaintext* kembali. Proses enkripsi dilakukan saat pengisian data dari suatu aplikasi ke dalam *smart card*, sedangkan proses dekripsi dilakukan saat pembacaan data dari *smart card* ke dalam suatu aplikasi.

Salah satu metode kriptografi untuk data berbentuk teks, seperti yang digunakan pada *smart card*, adalah AES (*Advanced Encryption Standard*). Metode kriptografi ini pertama kali dipublikasikan pada tahun 1998 dan diimplementasikan untuk melindungi pengiriman data berbentuk teks melalui jaringan internet secara global pada tahun 2002. AES sendiri diciptakan untuk menjadi standar global metode kriptografi data teks serta menggantikan metode kriptografi data teks lainnya, yaitu DES (*Data Encryption Standard*, mulai diimplementasikan sejak tahun 1978) dan 3DES (*Triple Data Encryption Standard*, pengembangan dari DES, mulai diimplementasikan sejak tahun 1991) yang dianggap telah usang dan rentan terhadap berbagai serangan terhadap metode kriptografi (*cryptanalysis*), seperti *brute – force attack*.[1][2][3]

Tugas Akhir ini akan membahas mengenai proses perancangan program berdasarkan metode kriptografi data teks AES dan melakukan implementasi program tersebut ke dalam dua buah aplikasi yang akan dibuat, yaitu aplikasi pengisian data *smart card* menggunakan metode enkripsi AES dan aplikasi pembacaan data *smart card* menggunakan metode dekripsi AES. *Smart card* yang digunakan adalah MIFARE Classic 1K dengan tipe *contactless smart card*. Perangkat *reader* yang akan digunakan berasal dari ACS (*Advanced Card Systems*), yaitu ACR1252U, yang berkomunikasi

dengan basis NFC (*Near Field Communication*). NFC sendiri merupakan pengembangan dari teknologi komunikasi nirkabel RFID (*Radio Frequency Identification*) dengan tipe HF (*High Frequency*) yang bekerja pada frekuensi 13,56 MHz dan digunakan sebagai medium oleh *smart card* serta *smart card reader* untuk saling berkomunikasi.

Parameter yang akan diteliti lebih lanjut dalam Tugas Akhir ini adalah performa dari metode kriptografi data teks AES yang akan dirancang dan diimplementasikan, yaitu waktu proses pengisian data *smart card* MIFARE Classic 1K menggunakan metode enkripsi AES dan pembacaan data *smart card* MIFARE Classic 1K menggunakan metode dekripsi AES. Metode kriptografi data teks AES yang akan digunakan adalah versi asli dan versi modifikasi (dengan pengubahan susunan nilai dalam S – Box dan IS – Box).

1.2 Identifikasi Masalah

Permasalahan yang akan dibahas dalam laporan ini adalah perancangan dan implementasi program berdasarkan metode kriptografi data teks AES dalam aplikasi pengisian data dan aplikasi pembacaan data *smart card* MIFARE Classic 1K dengan teknologi komunikasi berbasis NFC serta pengujian performa untuk proses enkripsi dan proses dekripsi AES di dalam aplikasi tersebut.

1.3 Rumusan Masalah

Masalah – masalah yang akan dibahas pada Tugas Akhir ini adalah :

- Bagaimana merancang aplikasi pengisian data dan aplikasi pembacaan data untuk *smart card* MIFARE Classic 1K dengan *reader* ACR1252U.
- Bagaimana merancang program enkripsi dan program dekripsi berdasarkan metode kriptografi data teks AES.

- Bagaimana mengimplementasikan program enkripsi AES ke dalam aplikasi pengisian data *smart card* dan program dekripsi AES ke dalam aplikasi pembacaan data *smart card*.
- Bagaimana melakukan prosedur *read* / *write* sehingga data dapat tersimpan dengan aman dalam *smart card* MIFARE Classic 1K.

1.4 Tujuan

Tujuan dari Tugas Akhir ini adalah :

- Mengimplementasikan metode kriptografi data teks AES ke dalam aplikasi pengisian data dan aplikasi pembacaan data untuk *smart card* MIFARE Classic 1K dan *reader* ACR1252U dengan teknologi komunikasi berbasis NFC.
- Meningkatkan keamanan pertukaran data antara *smart card*, terutama pada MIFARE Classic 1K, dengan perangkat *reader*.

1.5 Pembatasan Masalah

- *Smart card* yang digunakan adalah MIFARE Classic 1K dengan tipe *contactless smart card*.
- *Smart card reader* yang digunakan adalah ACR1252U yang bekerja dalam teknologi komunikasi berbasis NFC.
- Standar algoritma kriptografi data teks yang digunakan adalah AES dengan panjang *key* 128 bit (AES – 128).
- GUI (*Graphic User Interface*) untuk aplikasi pengisian data *smart card* dan aplikasi pembacaan data *smart card* dibuat menggunakan perangkat lunak Microsoft Visual Studio 2008 berbasis .NET.
- Bahasa pemrograman yang digunakan adalah C++.
- Pengujian performa metode kriptografi data teks AES yang akan dilakukan meliputi waktu proses pengisian data *smart card*

MIFARE Classic 1K menggunakan metode enkripsi AES dan waktu proses pembacaan data *smart card* MIFARE Classic 1K menggunakan metode dekripsi AES.

1.6 Metodologi Penelitian

Metodologi penelitian dalam Tugas Akhir ini adalah dengan cara eksperimental sehingga hasilnya dapat diuji. Langkah – langkahnya adalah :

- Mempelajari *datasheet* dari *reader* ACR1252U, *datasheet* dari *smart card* MIFARE Classic 1K dan bahasa pemrograman C++.
- Merancang program enkripsi dan dekripsi AES menggunakan bahasa pemrograman C++.
- Merancang aplikasi pengisian data *smart card* dan aplikasi pembacaan data *smart card* menggunakan bahasa pemrograman C++ berbasis .NET.
- Mengimplementasikan program enkripsi AES ke dalam aplikasi pengisian data *smart card* dan program dekripsi AES ke dalam aplikasi pembacaan data *smart card*.
- Menguji keberhasilan komunikasi berbasis NFC antara *smart card* dan *reader* serta proses enkripsi dan proses dekripsi AES di dalam aplikasi yang telah dibuat.

1.7 Spesifikasi Alat Yang Digunakan

- *Smart card reader* yang digunakan adalah ACR1252U NFC.
- *Smart card* yang digunakan adalah MIFARE Classic 1K dan bekerja berdasarkan prinsip ISO 14443 tipe A.
- Perangkat lunak yang digunakan adalah Microsoft Visual Studio 2008 berbasis .NET.

1.8 Sistematika Penulisan

Sistematika penulisan Laporan Tugas Akhir ini disusun menjadi lima bab, yaitu sebagai berikut :

BAB I : PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, identifikasi masalah, rumusan masalah, tujuan, pembatasan masalah, metodologi penelitian, spesifikasi alat dan sistematika penulisan Laporan Tugas Akhir ini.

BAB II : LANDASAN TEORI

Bab ini membahas teori – teori yang akan digunakan untuk merancang dan merealisasikan metode kriptografi data teks AES dalam aplikasi pengisian data dan aplikasi pembacaan data pada *smart card* MIFARE Classic 1K yang meliputi pembahasan tentang metode kriptografi data teks AES, teknologi komunikasi NFC, *smart card* MIFARE Classic 1K, *smart card reader* ACR1252U, Microsoft Visual Studio 2008 dan bahasa pemrograman C++.

BAB III : PERANCANGAN DAN REALISASI

Bab ini membahas perancangan dan implementasi proses enkripsi AES dalam aplikasi pengisian data dan proses dekripsi AES dalam aplikasi pembacaan data pada *smart card* MIFARE Classic 1K berbasis teknologi komunikasi NFC. Perancangan aplikasi disesuaikan dengan prosedur konfigurasi data yang dimiliki oleh *smart card* MIFARE Classic 1K.

BAB IV : DATA PENGAMATAN DAN ANALISA

Bab ini membahas tentang pengujian performa dari metode kriptografi data teks AES, yaitu waktu proses pengisian data dan pembacaan data *smart card* MIFARE Classic 1K menggunakan metode kriptografi data teks AES.

BAB V : SIMPULAN DAN SARAN

Bab ini merupakan bab penutup yang berisi simpulan hasil pengujian dan analisa dari Tugas Akhir ini serta saran untuk pengembangan lebih lanjut.