# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang Masalah

Teknologi s*mart card* atau kartu pintar menjadi salah satu aplikasi populer yang digunakan dalam aktivitas sehari-hari. Salah satu aplikasi berbasis *smart card* yang biasa digunakan di perguruan tinggi *smart campus* adalah sistem presensi. *Smart card* tersebut selain digunakan untuk tanda identitas, dia juga menyimpan data *civitas academica* di dalam kartu untuk sistem presensi. Saat ini sistem presensi di perguruan tinggi hanya berlaku untuk kalangan kampus itu sendiri. Sistem presensi tersebut tidak dapat membaca *smart card* yang berasal dari perguruan tinggi lain, karena tiap kampus memiliki kebijakan sistem keamanan yang berbeda-beda.

Keamanan data adalah hal yang penting dalam merancang suatu sistem elektronik, termasuk sistem presensi dengan *smart card*. Data dalam *smart card* harus dilindungi agar tidak terjadi kerusakan, seperti *corrupt, fault, clone* serta *hack* yang rentan terjadi ketika terjadi komunikasi antara *smart card* dengan terminal. Salah satu tipe serangan dalam sistem *smart card* adalah *man in the middle attack. Man in the middle attack* adalah suatu usaha pengambilan data secara illegal oleh pihak ketiga ketika terjadi proses komunikasi data antara *smart card* dengan *reader* melalui jaringan. Dikutip dari portal berita liputan6.com, pada tahun 2016 terjadi belasan kasus pembobolan ATM yang berhasil diungkap oleh kepolisian [13]. Modus yang dilakukan penyerang adalah dengan melakukan *skimming,* yakni aktivitas untuk mencuri data dari ATM untuk mengambil kendali atas rekening korban. Kasus *man in the middle attack* dan *skimming* merupakan serangan pada sistem *smart card* dengan mencuri data ketika terjadi komunikasi antara kartu dan *reader.*

Untuk mencegah kerusakan data dan serangan yang rentan terjadi maka dirancang suatu metode keamanan, salah satunya adalah dengan *secure access module*. *Secure Access Module* atau *Secure Application Module* (SAM) adalah perangkat keamanan data yang dapat diitegrasikan dengan *reader* untuk proses otentikasi atau validasi data yang disimpan dalam *smart card*. Algoritma kriptografi dan data penting seperti kunci akan disimpan dalam SAM. SAM memiliki beberapa

keunggulan, seperti operasi yang bersifat sensitif yang seharusnya dilakukan oleh terminal dapat dioperasikan oleh SAM sendiri. SAM mencegah terjadinya serangan dan kerusakan pada data. Meskipun penyerang berhasil mencuri data, data yang dicuri tersebut sulit untuk dibaca karena terenskripsi.

Pada tugas akhir ini, dilakukan tugas akhir implementasi *secure access module* sebagai sistem keamanan pada *smart card.* SAM akan berfungsi sebagai alat otentikasi untuk keamanan pada aplikasi baca dan tulis kartu yang dapat dikembangkan menjadi sistem presensi pada *smart campus.* Pada pengembangan selanjutnya, sistem keamanan SAM ini akan diintegrasikan dengan sistem presensi pada berbagai perguruan tinggi. SAM menyimpan sejumlah kunci dari berbagai sistem keamanan presensi, sehingga *smart card* dapat melakukan otentikasi pada alat presensi di perguruan tinggi yang beragam namun dengan sistem SAM yang terintegrasi.

## 1.2. Tujuan dan Manfaat

Tujuan dari pembuatan tugas akhir ini adalah:

1. Merancang arsitektur sistem keamanan data untuk aplikasi baca dan tulis kartu menggunakan fitur-fitur pada SAM.
2. Merancang skenario SAM untuk otentikasi data untuk pada sistem baca dan tulis *smart card.*

Manfaat dari pembuatan tugas akhir ini adalah dapat diimplementasikan sebagai sistem keamanan data pada aplikasi baca dan tulis kartu yang dapat dikembangkan menjadi sistem presensi berbasis *smart card.*

## 1.3. Rumusan Masalah

Berdasarkan latar belakang pada tugas akhir ini terdapat beberapa permasalahan, yaitu:

1. Bagaimana cara merancang arsitektur sistem keamanan data untuk aplikasi baca dan tulis kartu menggunakan fitur-fitur pada SAM?
2. Bagaimana merancang skenario SAM untuk otentikasi data untuk sistem baca dan tulis berbasis *smart card*?

## 1.4. Ruang Lingkup Masalah

Ruang lingkup masalah pada tugas akhir ini adalah:

1. *Smart card* yang digunakan adalah kartu Mifare Desfire EV1 dan SCard32.
2. Sistem keamanan yang dirancang adalah sistem otentikasi untuk program baca dan tulis kartu, yang akan dikembangkan sebagai aplikasi *smart campus.*
3. Metode otentikasi yang digunakan dalam pengujian adalah *mutual authentication.*
4. Algoritma kriptografi yang digunakan adalah DES dan 3DES.

## 1.5. Metode Penelitian

Penulisan tugas akhir ini menggunakan metode penelitian berikut:

1. Studi literatur dilakukan dengan cara mempelajari materi yang berkaitan dengan tugas akhir ini. Referensi yang digunakan untuk tugas akhir ini adalah jurnal, buku perkuliahan, dan situs resmi yang bisa dipercaya.
2. Perancangan alat dilakukan dahulu agar alat yang diinginkan sesuai dengan menggunakan *flowchart*.
3. Pengujian terhadap sistem yang dirancang apakah sesuai dengan yang diharapkan.
4. Pengambilan kesimpulan dari hasil pengujian dan percobaan.