1. Pendahuluan

1.1 Latar Belakang

Kartu tanda mahasiswa merupakan salah satu identitas penting bagi mahasiswa dalam menjalankan aktivitas perkuliahan dan kegiatan kampus lainnya. Namun, saat ini kartu tanda mahasiswa masih rentan terhadap tindakan kecurangan dan pemalsuan, seperti penyalinan kartu mahasiswa. Hal ini disebabkan oleh kurangnya sistem keamanan yang memadai pada kartu tanda mahasiswa. Oleh karena itu, perlu dilakukan penelitian untuk meningkatkan keamanan kartu tanda mahasiswa.

Tugas Akhir ini berfokus pada peningkatan keamanan kartu tanda mahasiswa dikarenakan kartu mahasiswa yang berbasis RFID dapat disalin dengan mudah menggunakan aplikasi MIFARE Classic Tool yang tersedia untuk ponsel Android dengan memanfaatkan fitur *Near Field Communication* atau yang disingkat NFC. Kartu tanda mahasiswa menggunakan kartu *Radio Frequency Identification* atau yang biasa disingkat RFID bertipe Mifare Classic 1K buatan perusahaan NXP Semiconductor, kartu ini menggunakan frekuensi 13.56 MHz dengan kapasitas memori sebesar 1KB dengan jarak dari pembaca hingga 100 mm. Kartu jenis ini biasa digunakan sebagai kartu akses, kartu karyawan, dan kartu transportasi umum[1]. Media kartu yang digunakan untuk menyimpan hasil salinan menggunakan kartu RFID dengan nomor seri EL-MF1WA-CNB, kartu ini berjalan di frekuensi 13.56 MHz dan memiliki besar memori 1 KB. Tidak seperti kartu RFID lainnya, kartu ini diciptakan untuk dapat ditulis ulang berkali-kali di sector 0 nya, sector 0 merupakan sector dimana UID disimpan.

Selain itu, ponsel Android dengan fitur NFC dapat dimanfaatkan untuk mensimulasikan kartu mahasiswa dengan memanfaatkan aplikasi Card Emulator PRO yang tersedia untuk ponsel Android. Aplikasi ini membutuhkan akses ROOT. Untuk menggunakan aplikasi ini, pengguna hanya perlu memasukkan UID kartu mahasiswa untuk dapat mensimulasikan kartu tersebut. Setelah berhasil, pengguna nantinya tinggal menempelkan ponselnya ke pembaca kartu mahasiswa dan akan terdeteksi sebagai kartu mahasiswa yang sah.

Penelitian ini bertujuan untuk meningkatkan keamanan kartu tanda mahasiswa dengan menggunakan sistem enkripsi *Advanced Encryption Standard* (AES)-128 dan teknologi *rolling code*. Dengan sistem enkripsi AES-128, data pada kartu tanda mahasiswa dienkripsi sehingga tidak dapat dibaca oleh orang yang tidak berwenang. Sedangkan teknologi *rolling code* menghasilkan kode acak yang berbeda setiap kali kartu digunakan. Kode acak ini memiliki panjang 6 karakter dengan gabungan antara angka dari 0 sampai 9 dan semua alfabet dari a hingga z, baik huruf besar ataupun kecil sehingga sulit bagi orang yang tidak berwenang untuk mengakses akses tersebut.

Melalui Tugas Akhir ini, diharapkan dapat dilakukan peningkatan pada sistem keamanan kartu tanda mahasiswa dengan mengimplementasikan enkripsi AES-128 dan *rolling code*. Dengan mengintegrasikan sistem enkripsi dengan kode tambahan yang selalu berubah setelah mahasiswa melakukan tap kartu, dapat mencegah dilakukannya penyalinan kartu mahasiswa.

1.2 Perumusan Masalah

Rumusan masalah pada Tugas Akhir ini adalah :

1. Bagaimana mengimplementasikan sistem keamanan berbasis enkripsi AES dan *rolling code* pada kartu tanda mahasiswa?
2. Apakah penerapan enkripsi AES dan *rolling code* pada kartu tanda mahasiswa menimbulkan beban komputasi yang berat atau tidak?

1.3 Tujuan

Tujuan yang ingin dicapai pada Tugas Akhir ini adalah :

1. Mengintegrasikan sistem keamanan kartu tanda mahasiswa berbasis enkripsi AES dan *rolling code* untuk melindungi data dan akses pengguna yang valid.
2. Mengevaluasi dampak penerapan enkripsi AES dan *rolling code* pada kartu tanda mahasiswa terkait waktu pemrosesan dan beban komputasi.

1.4 Metodologi Penelitian

Pada penelitian ini, diperlukan metodologi yang spesifik untuk menyelesaikan penelitian mengenai sistem keamanan kartu tanda mahasiswa berbasis *Advanced Encryption Standard* (AES) dan *rolling code*. Tahapan metodologi penelitian ini dijelaskan sebagai berikut:

- Identifikasi Masalah

  Pada tahap ini, dilakukan identifikasi terhadap kerentanan keamanan yang ada pada kartu tanda mahasiswa (KTM) saat ini. Fokus utama adalah pada masalah pemalsuan dan serangan *replay attack*. Tujuan dari penelitian ini juga ditentukan, yaitu meningkatkan keamanan KTM melalui implementasi enkripsi AES-128 dan teknologi *rolling code*.
- Studi Literatur

  Tahap ini melibatkan studi literatur yang mendalam mengenai teori dan aplikasi teknologi *Radio Frequency Identification* (RFID), *Near Field Communication* (NFC), serta algoritma enkripsi AES dan *rolling code*. Literatur yang dipelajari mencakup studi kasus serangan terhadap sistem RFID, solusi keamanan yang telah ada, dan teknologi *microcontroller* yang relevan untuk implementasi sistem keamanan KTM
- Perancangan Sistem

  Pada tahap ini, dilakukan perancangan sistem keamanan KTM yang mencakup:
  1. Perancangan perangkat keras untuk alat pembaca dan penulis kartu RFID.
  2. Perancangan perangkat lunak untuk mengimplementasikan enkripsi AES-128 dan *rolling code* pada data yang disimpan di KTM.
- Implementasi

  Tahap ini melibatkan implementasi dari sistem yang telah dirancang. *Microcontroller* digunakan untuk menulis data ke kartu RFID. Data yang ditulis mencakup *Universal Unique Identifier* (UID) kode acak yang dihasilkan oleh sistem *rolling code* dan telah dienkripsi menggunakan AES-128.
- Evaluasi

  Pada tahap ini, dilakukan evaluasi terhadap sistem yang telah dibuat. Pengujian dilakukan untuk memastikan bahwa sistem enkripsi dan *rolling code* berfungsi sesuai dengan desain dan mampu mencegah serangan *replay attack*. Hasil pengujian dianalisis untuk mengevaluasi efektivitas dan kinerja sistem keamanan KTM. Berdasarkan hasil evaluasi, disusun kesimpulan mengenai keberhasilan implementasi sistem keamanan berbasis AES-128 dan *rolling code* pada KTM.