

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini yang semakin maju dan pesat tentu sangat berpengaruh pada proses kegiatan sehari-hari terutama pada bidang pendidikan. Sistem absensi dalam kegiatan belajar mengajar pada suatu institusi pendidikan baik sekolah maupun perguruan tinggi, tentu saja memiliki siswa atau mahasiswa yang harus dicatat kehadirannya setiap hari. Pencatatan kehadiran ini lebih sering dikenal sebagai absensi. Di era perkembangan teknologi seperti sekarang ini, tidak menutup kemungkinan bahwa *QR Code* dapat dimanfaatkan untuk sistem absensi pada bidang pendidikan sehingga dapat meningkatkan akurasi dan keamanan data pada proses absensi di bidang pendidikan.

Pada era modern proses transaksi data memang terus meningkat dan berkembang hingga tidak menutup kemungkinan keamanan data sangat diperlukan dan dipertanyakan tentang kerahasiaan serta kekuatannya untuk melindungi data sensitif yang telah di bagikan melalui jaringan internet. Seiring perkembangan teknologi yang semakin maju dan pesat, jenis keamanan atau enkripsi data yang ada di dunia saat ini sudah sangat banyak, salah satunya penemuan baru yaitu enkripsi AES atau *Advanced Encryption Standard*. Algoritma kriptografi bernama *Advanced Encryption Standard* atau *Rijndael* yang didesain oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES (*Data Encryption Standard*) yang diadakan oleh NIST (*National Institutes of Standards and Technology*). (Fricles, 2013)

Algoritma AES (*Advanced Encryption Standard*) atau *Rijndael* adalah algoritma block chipper dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) yang merupakan

algoritma penerus dari algoritma DES (*Data Encryption Standard*) yang sudah dianggap masa berlakunya telah usai karena faktor keamanan yang semakin lama semakin mudah membobol kuncinya. Kunci DES yang sebesar 56-bit dianggap sudah tidak memadai lagi dikarenakan pada tahun 1998, 70 ribu komputer di internet berhasil membobol satu kunci DES dalam waktu 96 hari. Tahun 1999 kejadian yang sama terjadi lagi dalam waktu lebih cepat yaitu hanya dalam waktu 22 hari. (Didi Surian, 2006)

Pentingnya integritas dalam proses absensi karena apabila tidak terpenuhi maka dapat mengakibatkan terjadinya manipulasi data dan penghapusan terhadap data asli. Salah satu solusi untuk menghindari hal-hal tersebut perlu adanya tindakan enkripsi data kode nomor induk di dalam database, dengan menghasilkan *chiphertext* dari *plaintext*. Metode keamanan ini disebut dengan Kriptografi dan dapat diterapkan pada *QR Code*.

QR Code singkatan dari *Quick Response Code* adalah teknologi matriks dua dimensi yang mampu menyimpan berbagai jenis informasi di dalamnya. Informasi yang dapat ditampung oleh sebuah *QR Code* mencapai 7089 digit angka dan 4296 karakter *alphanumeric*. *QR-CODE* pertama kali diperkenalkan oleh Denso Wave kepada publik pada tahun 1994 dan dikembangkan yang langsung dipimpin oleh Masahiro Hara dan Atsushi Tano. Menurut penelitian menyimpulkan bahwa *QR-CODE* dapat menyimpan data yang lebih besar dalam ruang yang lebih kecil, melakukan koreksi kesalahan yang dapat diandalkan pada kecepatan, dan memiliki waktu respon yang lebih cepat. Otentikasi aman dapat dicapai dengan menggunakan algoritma penyembunyian dengan *QR-CODE*. (Dwi Qunita Putri Ambeq Paramarta 2018).

Android adalah sistem operasi untuk telepon seluler yang berbasis Linux. Android juga menyediakan platform terbuka bagi para pengembang guna menciptakan aplikasi mereka sendiri

untuk digunakan oleh bermacam peranti bergerak. Android merupakan sebuah sistem operasi untuk telepon seluler seperti halnya Symbian pada Nokia, Palm dan Windows Mobile yang sebelumnya sudah terlebih dahulu kita kenal selama ini. Sistem Android dipakai di telepon pertama kali pada tanggal 22 Oktober 2008 untuk HTC Dream. Pada beberapa bulan kemudian ditahun berikutnya Operating System Android sudah banyak sekali dipakai oleh berbagai jenis telepon seluler. Android disebut sebagai OS yang kuat, cepat dan juga sangat baik.

Berdasarkan alasan yang telah dipaparkan diatas, penelitian ini dibuat perancangan sistem Absensi mahasiswa dengan implementasi *QR-CODE* berbasis Android dengan enkripsi AES (*Advanced Encryption Standard*) guna untuk kepentingan proses belajar mengajar agar mengurangi kecurangan dalam hal absensi kehadiran mahasiswa. Dikarenakan kehadiran mahasiswa pada penilaian akhir matakuliah, terdapat nilai kehadiran mahasiswa itu sendiri, yang akan berpengaruh pada penilaian akhir yang diberikan oleh dosen.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka masalah pada penulisan skripsi ini dapat diuraikan sebagai berikut :

1. Bagaimana cara menerapkan Algoritma AES pada *QR Code* berbasis Android?.
2. Apakah kerahasiaan absensi mahasiswa dapat dijaga dengan menggunakan *QR Code*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk membuat kode absensi matakuliah menggunakan *QR Code* agar kerahasiannya dapat terjaga pada sistem absensi dan kehadiran mahasiswa mempunyai pengaruh untuk penilaian akhir.

1.4 Batasan Penelitian

Agar penulisan ini mengarah pada permasalahan yang ada, maka perlu adanya batasan masalah. Adapun batasan masalah pada penelitian ini adalah:

1. Penelitian tidak membahas hitungan matematis dari algoritma AES.
2. Penelitian berfokus pada sistem absensi mata kuliah Dasar-Dasar Pemrograman di Universitas Teknokrat Indonesia.
3. *QR-CODE* yang akan ditampilkan adalah hasil dari enkripsi nama mata kuliah.

1.5 Manfaat Penelitian

Manfaat Penelitian ini adalah :

1. Hasil dari penelitian ini digunakan untuk pihak Dosen pengampu mata kuliah Dasar Dasar Pemrograman dan Kampus Universitas Teknokrat Indonesia.
2. Dapat menjadi acuan untuk pengembangan lanjutan sistem absensi menggunakan teknologi *QR Code* dan algoritma AES (*Advanced Encryption Standard*).