BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada perkembangan teknologi yang semakin maju dan pesat saat ini akan tentu berpengaruh pada kemudahan-kemudahan yang diberikan dalam kehidupan sehari-hari terutama dalam bidang pemerintahan, perusahaan dan pendidikan, sekolah, universitas dan tempat lainnya. Sistem presensi dalam kegiatan belajar mengajar didalam suatu perguruan tinggi, tentu saja memiliki mahasiswa/mahasiswi yang harus dicatat setiap hari. Pencatatan kehadiran ini lebih sering dikenal sebagai presensi.

Di era modern seperti sekarang ini, tidak menutup kemungkinan bahwa QR Kode dapat dimanfaatkan untuk sistem presensi di perguruan tinggi sehingga dapat meningkatkan kerahasiaan dan akurasi. Enkripsi juga dapat digunakan melindungi data yang tersimpan pada perangkat penyimpanan seperti harddisk, CD atau flashdisk. Hal tersebut penting agar bila sewaktu-waktu laptop atau flashdisk kita dicuri, maka si pencuri tidak akan mampu mengakses data yang ada didalamnya.

Semakin hari proses transaksi data memang terus berkembang hingga tidak menutup kemungkinan keamanan data sangat di perlukan dan dipertanyakan untuk kekuatannya melindungi data sensitif yang telah di bagikan melalui internet. Banyak sekali jenis enkripsi atau keamanan data yang ada di dunia saat ini, salah satunya yang termasuk penemuan baru yaitu enkripsi AES atau Advanced Encryption Standard. Algoritma kriptografi bernama Rijndael yang didesain oleh oleh Vincent Rijmen dan John Daemen asal Belgia keluar sebagai pemenang kontes algoritma kriptografi pengganti DES yang diadakan oleh NIST (National Institutes of Standards and Technology) milik pemerintah Amerika Serikat. Pada

2006, AES merupakan salah satu algoritma terpopuler yang digunakan dalam kriptografi kunci simetrik.

AES (Advanced Encryption Standard) adalah lanjutan dari algoritma enkripsi standar DES (Data Encryption Standard) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga pada tanggal 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES.

Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. Keamanan merupakan faktor terpenting dalam evaluasi (minimal seaman triple DES), yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui. Di samping itu, AES juga harus dapat digunakan secara bebas tanpa harus membayar royalti dan juga murah untuk diimplementasikan pada smart card yang memiliki ukuran memori kecil.

AES juga harus efisien dan cepat (minimal secepat Triple DES) dijalankan dalam berbagai mesin 8 bit hingga 64 bit, dan berbagai perangkat lunak. DES menggunakan stuktur Feistel yang memiliki kelebihan bahwa struktur enkripsi dan dekripsinya sama, meskipun menggunakan fungsi F yang tidak invertibel. Kelemahan Feistel yang utama adalah bahwa pada setiap ronde, hanya setengah data yang diolah. Sedangkan AES menggunakan struktur SPN (Substitution Permutation Network) yang memiliki derajat paralelisme yang lebih besar, sehingga diharapkan lebih cepat dari pada Feistel.

AES ini merupakan algoritma block cipher dengan menggunakan sistem permutasi dan substitusi (P-Box dan S-Box) bukan dengan jaringan Feistel sebagaiman block cipher pada umumnya. Jenis AES terbagi 3, yaitu :

- AES-128
- AES-192
- AES-256

Pengelompokkan jenis AES ini adalah berdasarkan panjang kunci yang digunakan. Angka-angka di belakang kata AES menggambarkan panjang kunci yang digunakan pada tipa-tiap AES. Selain itu, hal yang membedakan dari masing-masing AES ini adalah banyaknya round yang dipakai. AES-128 menggunakan 10 round, AES-192 sebanyak 12 round, dan AES-256 sebanyak 14 round.

AES memiliki ukuran block yang tetap sepanjang 128 bit dan ukuran kunci sepanjang 128, 192, atau 256 bit. Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit. Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit).

Sedangkan Rijndael sendiri dapat mempunyai ukuran matriks yang lebih dari itu dengan menambahkan kolom sebanyak yang diperlukan. Blok chiper tersebut dalam pembahasan ini akan diasumsikan sebagai sebuah kotak. Setiap plainteks akan dikonversikan terlebih dahulu ke dalam blok-blok tersebut dalam bentuk heksadesimal. Barulah kemudian blok itu akan diproses dengan metode yang akan dijelaskan.

Kerahasiaan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Dapat diperoleh dengan memberi akses terbatas pada informasi atau dengan penyandian informasi sehingga tidak memiliki arti apapun bagi pihak yang tidak berhak tersebut. Jika kerahasiaan ini tidak terpenuhi, maka mengakibatkan adanya penyalahgunaan wewenang oleh pihak yang tidak sah.

Pentingnya integritas dalam sebuah absensi karena apabila tidak terpenuhi dapat mengakibatkan terjadinya manipulasi maupun

penghapusan terhadap data asli. Salah satu solusi untuk menghindari resiko penyerangan terhadap informasi presensi adalah dengan melakukan tindakan enkripsi data kode nomer induk di dalam database, dengan menghasilkan sebuah ciphertext dari plaintext nilai asli. Metode keamanan ini disebut dengan teknik kriptografi. Teknik kriptografi dapat diterapkan pada QR Code.

QR Code adalah perkembangan dari barkode atau kode batang yang hanya mampu menyimpan informasi secara horizontal sedangkan QR Code mampu menyimpan informasi lebih banyak, baik secara horizontal maupun vertical. Menurut penelitian saranya dkk (2016) menyimpulkan Kode QR dapat menyimpan data dalam jumlah yang lebih besar dalam ruang yang lebih kecil, melakukan koreksi kesalahan yang dapat diandalkan pada kecepatan yang lebih tinggi dan memiliki waktu respon yang lebih cepat. Otentikasi aman, dicapai dengan menggunakan algoritma penyembunyian data dengan QR Code.

Berdasarkan alasan yang telah dipaparkan diatas, pada penelitian ini dibuat aplikasi smart presensi menggunakan QR Code dengan enkripsi algoritma AES membantu menjaga kerahasiaan dan keaslian absensi.

1.2 Rumusan Masalah

Dengan latar belakang di atas, maka rumusan masalah dari penulisan skripsi ini dapat diuraikan sebagai berikut:

1. Apakah kerahasiaan kode presensi peserta dapat dijaga dengan menggunakan QR Code?
2. Bagaimana cara AES dalam membuat kode QR Code pada sistem presensi?

1.3 Tujuan

Tujuan dari penelitian ini adalah membuat kode presensi menggunakan QR Code agar kerahasiaannya dapat terjaga pada sistem presensi

1.4 Batasan Masalah

Untuk menghindari adanya kemungkinan semakin berkembangnya masalah, maka penelitian dalam laporan ini dibatasi oleh hal-hal sebagai berikut:

1. Penelitian berfokus pada sistem presensi untuk mahasiswa yang sedang menempuh ujian.
2. Penelitian tidak membahas hitungan matematis dari algoritme AES.
3. Proses bisnis yang dilakukan mencakup enkripsi dan dekripsi terhadap QR Code.

1.5 Manfaat Penelitian

Manfaaat yang dapat diperoleh dari penelitian ini adalah:

1. Pengguna dapat meningkatkan keamanan dan kerahasiaan sistem presensi melalui teknik kriptografi yang terenkripsi.
2. Pengguna dapat melakukan penyimpanan informasi smart presensi secara rahasia (*confidential*) tanpa diketahui orang lain.
3. Pengguna dapat menjaga keutuhan (*integrity*) presensi untuk menghindari upaya penyadapan, pembajakan, dan hal yang menyebabkan kebocoran dan manipulasi informasi melalui teknik kriptografi yang terenkripsi.

1.6 Sistematika Penulisan

Sistematika penulisan memberikan gambaran dan uraian dari penyusunan skripsi secara garis besar yang meliputi beberapa bab, antara lain:

BAB I PENDAHULUAN

Memuat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi kajian pustaka, referensi, dan sumber-sumber yang berhubungan dengan permasalahan dalam skripsi antara lain mengenai presensi, kriptografi, algoritma AES serta teori-teori lainnya sebagai dasar penulisan skripsi.

BAB III METODOLOGI PENELITIAN

Menjelaskan metode atau langkah-langkah yang digunakan dalam penulisan skripsi. Metode apa yang digunakan baik dalam penulisan, perancangan, implementasi, dan pengujian dari sistem yang dibangun.

BAB IV PERANCANGAN

Pada bab ini dijelaskan analisis dan perancangan aplikasi *presensi* dengan algoritme kriptografi AES yang dapat menjawab permasalahan yang telah diuraikan pada rumusan masalah.

BAB V IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas tentang implementasi sistem keamanan dan pengujian berdasarkan metode penelitian yang telah dibuat untuk diketahui hasilnya.

BAB VI PENUTUP

Bab ini memuat tentang kesimpulan yang diperoleh dari pembuatan dan pengujian aplikasi yang

dikembangkan dalam penelitian skripsi disertai saran yang dapat dijadikan masukan untuk pengembangan lebih lanjut.