

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dengan majunya perkembangan teknologi mempermudah memperoleh suatu informasi sangatlah mudah. Dan dengan berperannya teknologi di berbagai aspek kehidupan, salah satunya adalah *Radio Frequency Identification* (RFID). Teknologi RFID sudah banyak digunakan di kehidupan sehari-hari. Contohnya RFID digunakan sebagai sistem absensi, pembayaran, serta *Electronic Kartu Tanda Penduduk* (E-KTP).

Kriptografi adalah ilmu yang mempelajari cara mengamankan data dengan metode-metode yang ada. Sehingga data tertentu hanya dapat diakses oleh orang yang memiliki kuncinya saja.

Algoritma MD5 merupakan salah satu algoritma yang dikembangkan oleh Ron Rivest pada tahun 1991. Algoritma MD 5 mengambil inputan dengan panjang sembarang dan menghasilkan output berupa *digest*.

Algoritma RC4 dibuat oleh Ronald Rivest pada tahun 1984. RC4 merupakan sistem sandi stream berorientasi byte, dimana masukan RC4 sebuah byte dan kemudian dilakukan operasi XOR dengan sebuah byte kunci yang menghasilkan sebuah byte sandi.

Berdasarkan hal tersebut, penulis ingin mengimplementasikan algoritma MD5 dan algoritma RC4 untuk melakukan pengamanan data pada RFID. Sesuai

dengan bahasan diatas, maka untuk skripsi penyusun mengambil judul :
"Penerapan Algoritma MD5 dan Algoritma RC4 pada RFID"

1.2 Rumusan Masalah

Berdasarkan dari latar belakang di atas maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana membuat aplikasi untuk melakukan proses enkripsi dan deskripsi data pada *Radio Frequency Identification* (RFID), dengan algoritma MD5 dan algoritma RC4?

1.3 Batasan Masalah

Dalam pembuatan aplikasi ini, dibuat beberapa pembatasan masalah antara lain :

1. Aplikasi yang dibuat sebatas untuk melakukan proses enkripsi dan deskripsi.
2. Aplikasi yang dibuat berbasis desktop.
3. Aplikasi dibuat dengan menggunakan Visual studio dengan bahasa Visual C#.

1.4 Tujuan dan Maksud Penelitian

Tujuan dari penelitian ini diantara lain :

1. Untuk melakukan proses enkripsi dan deskripsi dengan menggunakan kombinasi 2 algoritma yaitu Algoritma MD5 dan Algoritma RC4

2. Hasil enkripsi algoritma MD5 digunakan sebagai *key* di algoritma RC4.
3. Algoritma RC4 digunakan sebagai hasil akhir enkripsi.

1.5 Manfaat Penelitian

Dari penelitian yang dilakukan dapat menghasilkan manfaat bagi pembaca dan penulis antara lain :

1. Dapat saling berbagai ilmu selama proses belajar di UNIVERSITAS Amikom Yogyakarta.
2. Bagi penulis, penulis mendapatkan pengalaman dari pembuatan kriptografi dengan menggunakan Algoritma MD5 dan Algoritma RC4.
3. Bagi pembaca, dapat menambah pengetahuan terhadap mengenai kriptografi.

1.6 Metode Penelitian

Dalam melakukan penelitian dan pembuatan skripsi ini, penulis mengumpulkan data melalui beberapa metode agar data yang terkumpul menjadi tepat, lengkap dan terstruktur. Metode – metode penelitian tersebut adalah :

1.6.1 Metode Pengumpulan Data

1.6.1.1 Metode Literatur

Metode literatur yaitu mencari referensi-referensi terkait seperti : buku, jurnal, dan referensi dari website yang digunakan dan teknis pengerjaan.

1.6.2 Metode Analisis

Pada tahap ini melakukan analisa terhadap algoritma yang digunakan. Algoritma yang di analisa adalah algoritma MD5 dan RC4.

1.7 Sistematika Penulisan

Dalam penulisan skripsi ini , penulis menjabarkan menjadi 5 bab, masing-masing diuraikan sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, pokok permasalahan, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penelitian yang disajikan secara terstruktur.

BAB II LANDASAN TEORI

Bab ini berisi dasar-dasar teori yang mendukung dalam melakukan analisa penelitian. Landasan teori merupakan rangkuman hasil studi literatur yang dilakukan oleh penulis untuk digunakan dalam penulisan skripsi ini.

BAB III ANALISA DAN PERANCANGAN SISTEM

Berisikan langkah-langkah penelitian yang dilakukan, pengimplementasian Algoritma, dan analisis terhadap algoritma MD5 dan RC4.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Berisikan Informasi tentang algoritma MD5 dan Algoritma RC4 dalam penerapannya, dan hasil akhir penelitian.

BAB V PENUTUP

Bab terakhir berisi mengenai kesimpulan dari semua yang telah diuraikan dan saran-saran yang dianggap perlu untuk mengatasi permasalahan yang terjadi.

DAFTAR PUSTAKA

LAMPIRAN

