BAB I
PENDAHULUAN

1.1 Latar Belakang

Sangat pentingnya nilai sebuah informasi menyebabkan sering kali informasi yang hanya boleh diakses oleh orang-orang tertentu, jatuh ke pihak lain sehingga dapat menimbulkan kerugian bagi pemilik informasi. Seperti password atau nomor kartu kredit. Atau pada aplikasi berbasis web, dalam hal ini aplikasi toko buku berbasis web. Dalam aplikasi ini biasanya bagian yang perlu dilindungi adalah password dan proses transaksi yang sedang berlangsung. Untuk memastikan bahwa pengguna adalah benar orang yang berhak, maka diperlukan sistem autentikasi. Ada beberapa metode untuk melakukan autentikasi, salah satunya yang umum dipakai adalah menggunakan password. Teknik yang digunakan adalah kriptografi.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Teknik kriptografi yang berkaitan dengan password adalah fungsi hash. Agar password lebih sulit dibobol, dirancang satu fungsi hash khusus yakni fungsi derivasi kunci. Sedangkan untuk pengamanan data kartu kredit dapat digunakan algortima DES.

DES atau juga dikenal sebagai *Data Encryption Algorithm*, merupakan algortima kriptografi simetris yang paling umum digunakan saat ini. DES merupakan blok cipher yang beroperasi dengan blok berukuran 64-bit dan kunci berukuran 56-bit.

Fungsi derivasi kunci yang pertama disebut CRYPT dibuat oleh Robert Tappan Morris, Sr. sekitar tahun 1980 untuk enkripsi password sistem UNIX. Fungsi ini

menggunakan 25 iterasi, salt 12 bit dan varian dari DES sebagai sub fungsi. Kemudian Poul-Henning Kamp membuat crypt MD5 untuk FreeBSD.

Crypt MD5 adalah salah satu fungsi derivasi kunci yang memproses input string password dan salt menggunakan perulangan algoritma MD5 untuk menghasilkan output. Algoritma Crypt MD5 ini menggunakan salt sepanjang 64 bit dan 1000 kali iterasi utama. Fungsi kompresi Crypt MD5 sama dengan fungsi kompresi MD5. Output utama yang dihasilkan sepanjang 132 bit dan menggunakan transformasi base64 untuk representasinya.

1.2 Perumusan Masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut :

a. Bagaimana mengimplementasikan algoritma crypt MD5 untuk pengamanan proses autentikasi password dan proses transaksi aplikasi toko buku berbasis web.
b. Bagaimana tingkat kemananan algoritma crypt MD5 dalam proses autentikasi password dan proses transaksi pada aplikasi toko buku berbasis web.

Adapun batasan masalah tugas akhir ini adalah :

a. Algoritma enkripsi yang dipakai adalah algoritma crypt MD5 dengan salt 64 bit dan 1000 kali iterasi utama.
b. Pada tugas akhir ini hanya akan dibahas mengenai proses autentikasi password dan nomor kartu kredit yang diinputkan oleh user dan simulasi proses transaksi.
c. Untuk simulasi proses transaksi dan pembayaran, pihak bank dan pihak ketiga sebagai validator kartu kredit adalah database.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah :

a. Membuat aplikasi toko buku berbasis web dengan mengimplementasikan algoritma crypt MD5 untuk proses autentikasi password untuk meningkatkan keamanan aplikasi.
b. Menganalisis performansi aplikasi toko buku berbasis web dengan algoritma crypt MD5 dibandingkan aplikasi dengan algoritma MD5 dari segi kecepatan proses enkripsi serta *response time* algoritma Crypt MD5.

1.4 Metodologi Penyelesaian Masalah

Metodologi pembahasan yang digunakan dalam penelitian Tugas Akhir ini adalah:

1. Studi literatur

   Mempelajari literatur–literatur yang relevan dengan permasalahan yang meliputi : fungsi hash, algoritma message diggest, fungsi derivasi kunci, algoritma crypt MD5, Macromedia Dreamweaver MX, PHP, JavaScript dan MySQL.

2. Analisis Masalah dan Perancangan Perangkat Lunak

   Identifikasi kebutuhan dan spesifikasi yang ingin dibuat didalam perangkat lunaknya sehingga mempermudah pembangunan aplikasi, yaitu merancang aplikasi toko buku berbasis web dengan menggunakan Macromedia Dreamweaver MX serta PHP, JavaScript dan MySQL.

3. Implementasi dan Pembangunan Perangkat Lunak
   - Menerjemahkan perancangan system menjadi bahasa pemrograman. Adapun bahasa pemrograman yang dipakai adalah PHP dan JavaScript.
   - Implementasi aplikasi yakni dengan mengimplementasikan algoritma crypt MD5 pada aplikasi toko buku berbasis web.

4. Pengujian dan Analisis hasil aplikasi
    - Melakukan pengujian proses autentikasi password dan nomor kartu kredit pada aplikasi toko buku berbasis web dengan membandingkan hasil enkripsi yang diinputkan oleh user dengan data pada database.
    - Melakukan analisa perbandingan keamanan proses autentikasi password setelah pengimplementasian algortima crypt MD5.

5. Penyusunan laporan tugas akhir dan kesimpulan akhir.