BAB I

PENDAHULUAN

1.1. Latar Belakang

Dalam perkembangan pemrograman internet terdapat banyak jenis bahasa pemrograman yang pembuat aplikasi kenal baik pemrograman di sisi server maupun pemrograman di sisi klien. Sebut saja bahasa pemrograman PHP (PHP Hypertext Preprocessor), JSP (Java Server Pages), ASP (Active Server Pages), HTML (HyperText Markup Language), XHTML (eXtensible HyperText Markup Language), dan lain sebagainya. Namun tetap saja kode yang diterjemahkan oleh browser itu berupa halaman HTML (HyperText Markup Language).

Namun kode asal halaman HTML dapat dengan mudah dilihat oleh semua orang dengan melakukan view page source pada browser. Keamanan halaman web sangat di butuhkan karena dapat menimbulkan pencurian kode dan Jenis pencurian kode dapat bermacam-macam, mulai dari mencuri desain web, membobol sistem keamanan yang berbasis JavaScript, menyalin konten yang seharusnya tidak boleh disalin seperti alamat referensi sumber

berkas atau mengambil sumber data dari database yang telah di link pada halaman web.

Terkadang web programmer sering mengabaikan faktor keamanan dalam halaman HTML yang dapat mengakibatkan munculnya kerusakan atau kerugian. Contoh yang paling mudah adalah melakukan validasi dengan menggunakan pemrograman sisi pengguna sehingga dalam halaman web akan terdapat password yang akan dengan mudah bisa dilihat hanya dengan melakukan view page source.

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan algoritma kriptografi DES (Data Encryption Standard) untuk proses enkripsi dan deskripsi data. Kriptografi telah menjadi suatu bagian yang tidak dapat di pisahkan dari sistem keamanan jaringan, Salah satu metode enkripsi data adalah Data Encryption Standard (DES). DES dapat dioperasikan dengan metode CBC (Cipher Block Chaining). Dengan menggunakan metode CBC kriptanalisis menjadi lebih sulit dikarenakan blok-blok plainteks yang sama tidak menghasilkan blok-blok cipherteks yang sama.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas dapat dirumuskan yaitu, bagaimana membuat aplikasi pengamanan halaman web berbasis HTML dengan menggunakan algoritma enkripsi DES (Data Encryption Standard) metode CBC (Cipher Block Chaining).

1.3. Ruang Lingkup Masalah

Ruang lingkup dari penelitian dan pembuatan aplikasi ini adalah:

1. Aplikasi yang akan dibuat diimplementasikan pada kode halaman web dengan berbasis HTML,SHTML dan XHTML. Perbedaan antara XHTML dan HTML adalah XHTML merupakan versi diatas HTML, penulisan kode menggunakan bahasa XHTML haruslah disusun secara rapi dan tertib. Semua elemen pembuka pada XHTML harus ditutup, ini berbeda dengan HTML sedangkan SHTML(Secure Hypertext Markup Language) yang merupakan ektensi dari file SSI(Server Side Include) yaitu sebuah metode untuk memasukkan konten dari sebuah file ke file lainnya.

2. Metode enkripsi yang digunakan untuk pengamanan halaman web dibatasi pada penggabungan algoritma enkripsi DES (Data Encryption Standard) dengan metode CBC (Cipher Block Chaining).

1.4. Tujuan Penelitian

Dari perumusan masalah diatas penelitian ini bertujuan untuk membuat sebuah aplikasi pengamanan halaman web HTML dengan menggunakan algoritma enkripsi DES (Data Encryption Standard) dengan metode CBC (Cipher Block Chaining). berbasis bahasa pemrograman java desktop(Java SE).