BAB I
PENDAHULUAN

1.1 Latar Belakang

Bertukar informasi/data di jaman teknologi yang sudah sangat berkembang pesat seperti saat ini umum dilakukan oleh berbagai pihak, dalam bertukar data pihak pengirim dan penerima terkadang mengenyampingkan hal keamanan dan kerahasiaan. Seiring dengan itu, kebutuhan pada keamanan terhadap kerahasiaan data yang saling dipertukarkan tersebut semakin meningkat. Oleh karena itu dikembangkan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, keamanan merupakan bentuk tindakan untuk mempertahankan suatu hal dari berbagai macam gangguan dan ancaman. Terdapat banyak faktor yang mengancam keamanan komunikasi data. Ancaman-ancaman tersebut menjadi masalah terutama dengan semakin meningkatnya komunikasi data yang bersifat rahasia.

Selama ini aplikasi yang dapat melakukan enkripsi *file* yang berbasis web belum tersedia. Hanya tersedia dalam bentuk aplikasi *offline*. Seperti aplikasi enkripsi dan dekripsi dengan menggunakan algoritma MD5 dan aplikasi enkripsi dan dekripsi dengan algoritma RSA. Kedua metode tersebut cukup memiliki tingkat kerahasiaan dan algoritma tersendiri dalam menjadikan sebuah *plaintext* menjadi *ciphertext.*

Algoritma *Cipher Block Chaining* merupakan penerapan mekanisme umpan balik pada sebuah blok *bit* dimana hasil enkripsi blok sebelumnya diumpan balikkan ke dalam proses enkripsi blok *current.* Caranya, blok *plaintext* yang *current* di-XOR-kan terlebih dahulu dengan blok *ciphertext* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma CBC, setiap blok *ciphertext* tidak hanya bergantung pada blok *plaintext* tetapi juga pada seluruh blok *plaintext* sebelumnya.

Pemberian fasilitas enkripsi dan dekripsi dengan algoritma kriptografi *Cipher Block Chaining* (CBC) ke dalam sebuah web portal ini dilakukan karena metode ini diimplementasikan pada level *binary digit* (*bit*), sehingga pola proses enkripsi tidak dapat terbaca, serta proses enkripsi dan deskripsi memerlukan waktu singkat.

1.2 Rumusan Masalah

Dari uraian yang dikemukakan pada latar belakang, dapat dirumuskan masalah – masalah sebagai berikut :

1. Bagaimana membuat sebuah web yang menyediakan fasilitas enkripsi dan deskripsi dengan algoritma *Cipher Block Chaining* (CBC)
2. Berapa tingkat akurasi pengembalian atau deskripsi kalimat yang telah dienkripsi.

1.3 Tujuan

Adapun tujuan penulis melakukan penelitian ini adalah :

1. Membuat portal *online* penyedia fasilitas enkripsi dan dekripsi dengan metode *Cipher Block Chaining* (CBC) dengan menggunakan Bahasa pemrograman PHP dan MySQL
2. Mengukur keakurasian pengembalian atau deskripsi dari kalimat yang telah terenkripsi

1.4 Batasan Masalah

Agar pembahasan tidak menyimpang dari topik permasalahan yang ada, maka penulis membuat batasan masalah dalam penelitian ini, antara lain :

1. Data/*file* yang akan dienkripsi terdiri dari *file* teks (*.txt), file dokumen (*.docx), dan *file* gambar (*.jpg) dan (*.png).
2. Ukuran *file* gambar yang akan diproses tidak lebih dari 600 x 600 *pixels*.
3. Isi *file* *.docx yang dienkripsi tidak mengandung unsur tabel dan gambar.
4. *File* gambar (*.jpg dan *.png) yang dienkripsi adalah data *bit*-nya, bukan warna.

1.5 Manfaat

Manfaat dari pembangunan portal online ini dapat digunakan untuk menjaga kerahasiaan *file*/data dengan proses enkripsi dan dekripsi menggunakan algoritma *Cipher Block Chaining* (CBC) sebelum melakukan pengiriman atau berbagi *file*/data melalui media pengiriman data.