ABSTRAK

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.

Algoritma *Cipher Block Chaining* (CBC) 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.

Web portal yang terbentuk telah dapat menyediakan fasilitas enkripsi dan dekripsi pada *file* *.docx, *.txt, *.jpg dan *.png menggunakan algoritma *Cipher Block Chaining* (CBC) dengan tingkat akurasi pengembalian kalimat (*.docx dan *.txt) pada 3 skenario (10, 50 dan 150 kata) pengujian adalah 100%, serta akurasi pengembalian ukuran *pixels* dan ukuran *file* (*.jpg dan *.png) dari 3 kali pengujian pada 3 *file* dengan ukuran *pixels* dan ukuran *file* yang berbeda adalah 100%. Namun tidak dapat mengembalikan gambar dan tabel yang terdapat pada *file* *.docx.

Kata Kunci : Kerahasiaan dan Keamanan, Pengiriman Data, *Cipher Block Chaining* (CBC)

ABSTRACT

Secrecy and security data is of crucial importance in communication data, security is a form of action to maintain a thing of various disorder and threat.There are many factors that threatens security data communication. Threats become the problem especially with the increase data communication that are secret.

Cipher Block Chaining algorithm is an implementation of a feedback mechanism at a result bit block encryption block previously routed invert into the encryption process blocks current. Here's how the current plaintext block, XOR operation advance with blocks of ciphertext encryption results results of previous, next it was entered in XOR operation to the function of encryption. CBC algorithm, with each block of ciphertext depends not only on the block of plaintext but also on the entire plaintext block before.

*Web portal that is formed has been able to provide encryption and decryption facilities in the * .docx, * .txt, * .jpg, and * .png algorithm using Cipher Block Chaining (CBC) with the accuracy of the return of the sentence (* .docx and * .txt) at 3 scenarios (10, 50 and 150 words) the test was 100%, and accuracy of the return of the size of pixels and the size of the files (* .jpg, and * .png) of 3 times the test on three files with a size of pixels and a different file size is 100 %. Yet it can not restore images and tables contained in the file * .docx.*

Keywords : Confidentiality and security, Shipping Data, Cipher Block Chaining (CBC)