Portal *Online* Penyedia Fasilitas Enkripsi dan Dekripsi Menggunakan Metode *Cipher Block Chaining* (CBC)

Hari Setiady Wibowo (1210651167)[1]
Taufiq Timur W, S.Kom, M. Kom[2]
Jurusan Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Jember
Jln. Karimata No. 49, Telp (0331) 336728, Jember
E-mail : harisetiadyw@gmail.com

Abstract

Exchange of information/data on the age of the technology which is already very rapidly growing public as currently carried out by various parties, in exchanging data sender and recipient parties sometimes throw over it security and confidentiality. Along with that, the need for security against the confidentiality of the data exchanged. Therefore developed branch of science that studies about ways of data security or Cryptography terms known.

Keyword : Data sender, Security and Cryptography

Abstrak

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.

Kata kunci : Pengiriman data, Keamanan dan Kriptografi

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.

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 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. Bagaimana tingkat akurasi pengembalian atau dekripsi *file* yang telah di enkripsi

2.2 Batasan Masalah

Agar pembahasan tidak menyimpang dari topik 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. *File* *.docx akan di *encode* dengan *base64*.
3. Isi *file* *.docx yang dienkripsi tidak mengandung unsur tabel dan gambar.

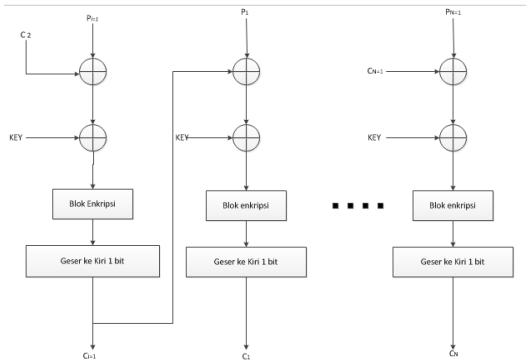
II TINJAUAN PUSTAKA

2.1 Kriptografi

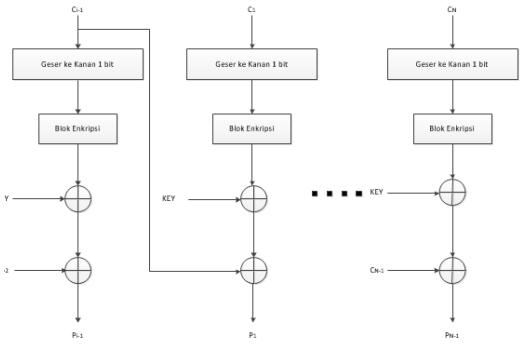
Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi pengiriman pesan dan tanda tangan digital dan kieaslian pesan dengan sidik jari digital dan keaslian pesan dengan sidik jari digital (Ariyus, 2005).

2.2 *Cipher Block Chaining* (CBC)

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. Dekripsi dilakukan dengan memasukkan blok *ciphertext* yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok *ciphertext* sebelumnya. Dalam hal ini, block *ciphertext* sebelumnya berfungsi sebagai umpan maju (*feedforward*) pada akhir proses deskripsi. (Rosmala, 2012)



Gambar 2.1 Skema enkripsi dengan algoritma CBC



Gambar 2.2 Skema dekripsi dengan algoritma CBC

III METODOLOGI PENELITIAN

3.1 Analisis Metode

Pada proses enkripsi data, akan digunakan algoritma *Cipher Block Chaining* (CBC). Pada enkripsi *Cipher Block Chaining* (CBC) dimulai dengan proses membagi *plaintext* menjadi blok yang telah *ditentukan* ukurannya, pada sistem aplikasi ini tiap blok berukuran 128 bit. Satu blok *plaintext* yang telah dibagi di-XOR-kan dengan IV (*Initialization Vector*) yang telah ditentukan, kemudian hasil tersebut di-XOR-kan lagi dengan kunci. Hasil XOR tersebut digeser 1 *bit* ke kiri, hasil tersebut menjadi IV untuk blok berikutnya. Proses diulang sampai blok berakhir.

3.2 Proses Enkripsi

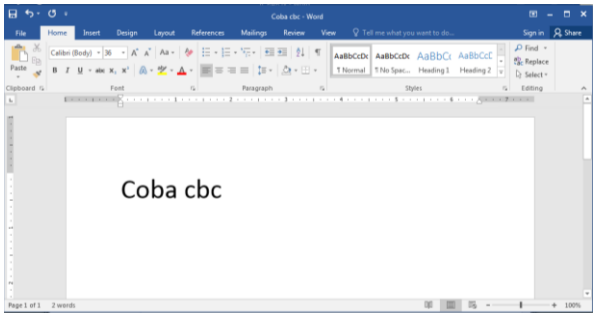
Plainteks : HARISETIADY
IV : K (01001011)
Kunci : V (01010110)
P1 = 01001000,01000001,01010010,
01001001,01010011,01000101,
01010100,01001001,01000001,
01000100,01011001
$C_0 = P1 \oplus IV$
C0 = 0000011,00001010,00011001,
00000010,00011000,00001110,
00011111,00000010,00001010,
00001111,00010010
$C_1 = C_0 \oplus K$
C1 = 01010101,01011100,01001111,
01010100,01001110,01011000,
01001001,01010100,01011100,
01011001,01000100

C1 digeser 1 bit ke kiri
C1 = 10101010,10111000,10011110,
10101000,10011100,10110000,
10010010,10101000,10111000,
10110010,10001000
Ciphertext = ª‚Ž¨œ°˜™ ¸²ˆ

IV IMPLEMENTASI

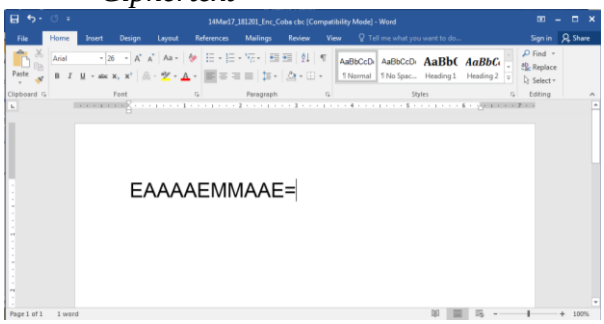
4.1 Implementasi Pada *File* *.docx

Plaintext



Gambar 4.1 *File* *.docx sebelum dienkripsi

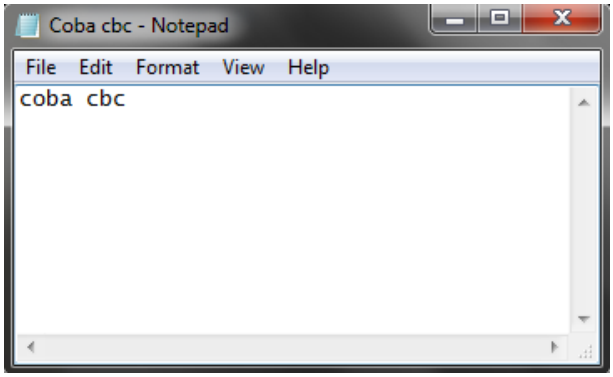
Ciphertext



Gambar 4.2 *File* *.docx setelah dienkripsi

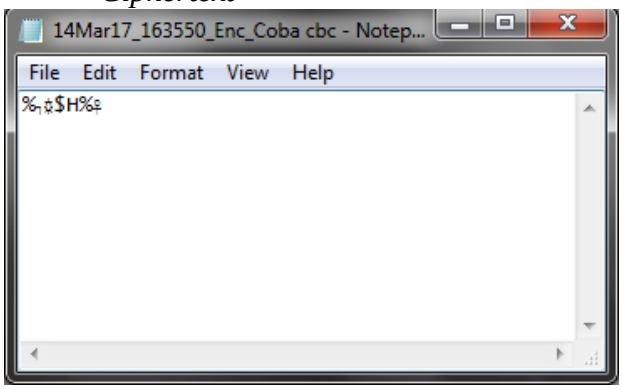
4.2 Implementasi *File* *.txt

Plaintext



Gambar 4.3 *File* *.txt sebelum dienkripsi

Ciphertext



Gambar 4.4 *File* *.txt setelah dienkripsi

4.3 Implementasi *File* *.jpg

Plaintext

Gambar 4.5 *File* *.jpg sebelum dienkripsi

Ciphertext

Gambar 4.6 *File* *.jpg setelah dienkripsi

4.4 Implementasi Pada *File* *.png

Plaintext

Gambar 4.7 *File* *.png sebelum dienkripsi

Ciphertext

Gambar 4.8 *File* *.png setelah dienkripsi

V KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan implementasi didapatkan kesimpulan :

1. Web portal yang terbentuk telah dapat menyediakan fasilitas enkripsi dan dekripsi dengan menggunakan metode *Cipher Block Chaining* (CBC)
2. Fasilitas enkripsi dan deskripsi pada web portal ini dapat mengembalikan file dalam format *.txt, *.docx, *.jpg dan *.png seperti pada saat sebelum di enkripsi.
3. *File* *.docx yang dienkripsi atau didekripsi akan di *encode base64* dan *decode base64* agar tidak merubah *content* dalam *file*.
4. *File* *.docx yang mengandung unsur gambar dan tabel, gambar dan tabel tidak terdekripsi secara sempurna.
5. *File* *.jpg dan *.png terenkripsi menjadi file yang tidak dapat terlihat isi gambarnya.

5.2 Saran

Berdasarkan implementasi, didapatkan saran :

1. Agar dapat dikembangkan dengan menambah ekstensi *file* yang dapat di enkripsi maupun didekripsi.
2. Dapat dikembangkan pada sistem operasi *android* atau *iOS.*

DAFTAR PUSTAKA

Rudianto,A. M. (2011). *Pemrograman Web Dinamis Menggunakan Php dan Mysql*. ANDI, Yogyakarta.

Lutfillah, F. (2015). *Implementasi Kriptografi Blowfish Pada Sebuah Informasi Dalam Bentuk QR Code*. Universitas Muhammadiyah Jember, Jember.

Mardianto. (2010). *Enkripsi Curve Cryptography (ECC).* Institut Teknologi Telkom, Bandung.

Munir, R. (2006). *Kriptografi.* Informatika, Bandung.

Purwono. (2009). *Buku Materi Pokok: Dasar-dasar Dokumentasi*. Universitas Terbuka. Modul 1, Jakarta.

Putra, D. (2010). *Pengolahan Citra Digital.* ANDI, Yogyakarta.

Rosmala, D. (2012). *Implementasi Mode Operasi Cipher Block Chaining (CBC) Pada Pengamanan Data.* Institut Teknologi Nasional Bandung, Bandung.

Wisnu, R. (2008). *Implementasi Algoritma RC6 Untuk Enkripsi SMS pada Telepon Seluler.* Institut Teknologi Bandung, Bandung.