

Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Cipher Block Chaining

Devi Andriani

Teknik Informatika STMIK Budidarma Medan; Jl. Sisingamangaraja No. 338 Medan
email :deviandri20@yahoo.co.id

Abstrak

Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, baik dengan tujuan keamanan bersama, maupun untuk privasi individu. Para pengguna komputer yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyasiasi cara mengamankan informasi yang akan dikomunikasikan atau yang akan disimpan. Perlindungan terhadap kerahasiaan data meningkat, salah satu caranya dengan menerapkan ilmu kriptografi.

Kriptografi adalah salah satu ilmu yang digunakan untuk menjaga kerahasiaan dan keamanan data sudah berkembang sejak jaman Yunani kuno. Kriptografi semakin berkembang dari jaman kejaman sampai saat ini. Salah satu metode kriptografi yang cukup handal, stabil dan menjadi induk dari algoritma – algoritma kriptografi yang populer saat ini adalah Cipher Block Chaining (CBC).

Cipher Block Chaining (CBC), mode ini merupakan mekanisme umpan balik (feedback) pada sebuah blok, dan dalam hal ini hasil enkripsi blok sebelumnya di umpan balikkan kedalam enkripsi blok yang current. Caranya, blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk kedalam fungsi enkripsi. Dengan algoritma Cipher Block Chaining (CBC), setiap blok ciphertext bergantung tidak hanya pada blok plainteks nya tetapi juga pada seluruh blok plainteks sebelumnya.

Perancangan Aplikasi algoritma Cipher Block Chaining (CB) dalam penelitian ini dilakukan dengan menggunakan aplikasi yang dibangun menggunakan bahasa pemograman Visual Studio 2008.

Kata Kunci : Kriptografi, PenyandianTeks, Algoritma Cipher Block Chaining

Abstract

Confidentiality and data security are very important in data communications, both with shared security objectives, as well as for individual privacy. Computer users who want the data unknown to unauthorized parties are always trying to get around how to secure the information to be communicated or to be stored. Protection of data confidentiality increases, one way to apply cryptography. Cryptography is one of the sciences used to maintain the confidentiality and security of data has evolved since ancient Greece. Cryptography has evolved from the age of cruelty to the present. One of cryptographic methods that is quite reliable, stable and the parent of the most popular cryptographic algorithms today is Cipher Block Chaining (CBC). Cipher Block Chaining (CBC), this mode is a feedback mechanism on a block, and in this case the previous block encryption results in feedback into current block encryption. The trick, the plaintext block is now XOR-first with the previous ciphertext block of encryption results, then the XOR-this results into the encryption function. Application Design of Cipher Block Chaining

(CB) algorithm in this research is done by using application built using Visual Studio programming language 2008.

Keywords: Cryptography, Text Encoding, Cipher Block Chaining Algorithm

1. PENDAHULUAN

Penyandian teks merupakan ilmu yang berdasarkan pada teknik informatika yang bertujuan untuk mengamankan informasi seperti kerahasiaan data dan otentik entitas. Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, baik dengan tujuan keamanan bersama maupun untuk privasi individu. Para pengguna computer yang menginginkan datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha meniasati cara mengamankan informasi yang akan dikomunikasikan atau yang akan disimpan. Sehingga perlindungan terhadap kerahasiaan meningkat, salah satu cara adalah penyandian dengan enkripsi. Enkripsi merupakan suatu proses pengubahan pesan asli menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang bisa digunakan seperti *Stream Cipher*, *Data Encryption Standard (DES)*, *Triple DES*, *Advanced Encryption Standard (AES)* dan sebagainya. Proses untuk mengembalikan pesan kedalam bentuk pesan yang asli disebut depenelitian.

2. METODE PENELITIAN

Dalam penyusunan laporan dibutuhkan data yang sangat akurat dan objektif agar dapat dilaksanakan pembahasan dan pengevaluasian serta penyimpulan untuk lebih mengerti dan memahami isi dari penyusunan laporan tersebut. Di dalam pengumpulan data yang akurat ini, penulis menggunakan beberapa metode untuk memperoleh data tersebut.

2.1 Penyandian Teks

Penyandian teks adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentik entitas (Nurli Hairiah, 2015, 138). Oleh karenanya dibutuhkan suatu proses penyandian atau pengkodean data. Sehingga data dapat terjaga kerahasiaannya dan tidak dapat dengan mudah diubah untuk menjaga integritas data tersebut. Untuk menjamin keamanan dan keutuhandari suatu data, dibutuhkan suatu proses penyandian.

2.2 Kriptografi

Cryptography (kriptografi) berasal dari bahasa Yunani yaitu dari kata *crypto* yang berarti penulisan *secret* (rahasia), sedangkan *graphein* artinya *writing* (tulisan). Jadi secara sederhana dapat diartikan *secret writing* (tulisan rahasia). Definisi lain dari kriptografi adalah sebuah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi (Rinaldi Munir, 2006) yaitu:

1. Kerahasiaan (*confidentiality*), adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data (*data integrity*), adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak,

antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang kebenarnya.

3. Outentikasi (*authentication*), adalah usaha yang berhubungan dengan identifikasi/pengenalan, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4. *Non-repudiasi* adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

2.3 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut (Dony Arius, 2006). Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

1. Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai *cipher* atau kode dengan menggunakan algoritma yang untuk mengkodekan data yang diinginkan.
2. Dekripsi merupakan kebalikan dari proses enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekritpsi pesan. Algoritma yang digunakan untuk dekritpsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekritpsi. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Berdasarkan kunci yang dipakai dalam proses kriptografi, maka algoritma kriptografi dibagi menjadi [4] :

1. Algoritma Simetri ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekritpsi. Bila mengirim pesan dengan menggunakan algoritma ini, sipenerima pesan harus diberitahu kunci dari pesan tersebut agar bias mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Algoritma yang menggunakan kunci simetris misalnya DES, Kode Rivest's, IDEA, AES, OTP, A5 dan lain-lain
2. Algoritma Asimetris sering juga disebut dengan algoritma kunci public, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekritpsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian yaitu kunci umum (*public key*) yang bias diketahui oleh umum dan kunci rahasia (*private key*) yaitu kunci yang dirahasiakan dan hanya boleh diketahui oleh satu orang saja.
3. Fungsi Hash sering disebut dengan fungsi has satu arah (*one way function*), *message digest*, *fingerprint*, fungsi kompresi dan *Message Authentication Code* (MAC) yang merupakan suatu fungsi matematika yang mengambil masukan panjang variable dan mengubahnya kedalam urutan biner dengan panjang yang tetap.

2.4 Algoritma Kriptografi Modren

Kriptografi modern menggunakan gagasan dasar yang sama seperti kriptografi klasik (permutasi dan transposisi) tetapi penekanannya berbeda. Pada kriptografi klasik, kriptografer menggunakan algoritma yang sederhana, yang memungkinkan cipherteks dapat dipecahkan dengan mudah (melalui penggunaan statistic, tekaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit memecahkan

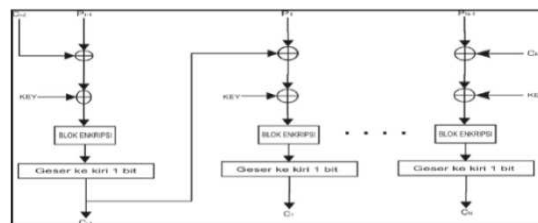
ciperteks tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi dalam mode *bit* ketimbang mode karakter (seperti yang dilakukan pada *cipher* substitusi atau *cipher* transposisi dari algoritma kriptografi klasik).

Operasi dalam mode *bit* berarti semua data dan informasi (baik kunci, plainteks, maupun ciperteks) dinyatakan dalam rangkaian (*string*) *bit* biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian *bit*. Rangkaian *bit* yang menyatakan plainteks dienkripsi menjadi ciperteks dalam bentuk rangkaian *bit*, demikian sebaliknya. Perkembangan algoritma kriptografi modern berbasis *bit* didorong oleh penggunaan komputer digital yang mempresentasikan data dalam bentuk biner (Rinaldi Munir, 2006).

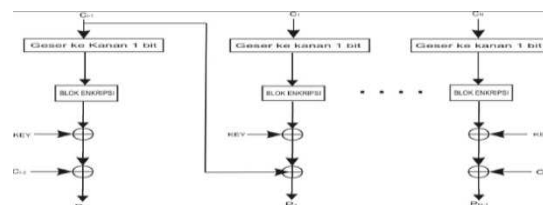
2.5 Algoritma Cipher Block Chaining

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*nya 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. Blok *ciphertext* sebelumnya berfungsi sebagai umpan maju (*feedforward*) pada akhir proses dekripsi (Dewi Rosmala, 2012, 58).



Gambar 1 Skema Enkripsi dengan Algoritma Cipher Block Chaining



Gambar 2 Skema Dekripsi dengan Algoritma Cipher Block Chaining

Secara matematis, enkripsi dan dekripsi dengan algoritma CBC [8] dinyatakan sebagai:

$$C_i = Ek(P_i \oplus C_{i-1})$$

$$P_i = Dk(C_i \oplus C_{i-1})$$

Enkripsi blok pertama, $C_0 = IV$ (*Initialization Vector*). *IV* dapat diberikan kepada pengguna atau dibangkitkan secara acak oleh program jadi, untuk menghasilkan blok *ciphertext* pertama (C_1), *IV* digunakan untuk menggantikan blok *ciphertext* sebelumnya. Sebaliknya pada dekripsi blok *plaintext* pertama diperoleh dengan cara meng-XOR-kan *IV* dengan hasil dekripsi terhadap blok *ciphertext* pertama (Rinaldi Munir, 2006). *IV* tidak perlu rahasia, jadi untuk *m* buah blok *plaintext*, enkripsinya adalah:

$$C_1 = Ek(P_1 \oplus IV)$$

$$C_2 = Ek(P_2 \oplus C_1)$$

$$C_3 = Ek(P_3 \oplus C_2)$$

$$C_m = Ek(P_m \oplus C_{m-1})$$

Dekripsi m buah blok *ciphertext* adalah:

$$\begin{aligned} P1 &= Dk (C1) \oplus IV \\ P2 &= Dk (C2) \oplus C1 \\ P3 &= Dk (C3) \oplus C2 \\ &\bullet \\ C_m &= Dk (C_m) \oplus C_{m-1} \end{aligned}$$

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Sistem ini dibuat dengan tujuan mengimplementasikan enkripsi dan dekripsi teks berdasarkan algoritma *Cipher Block Chaining* (CBC) dengan tujuan dapat memperlihatkan prosedur dan hasil yang didapatkan untuk mengamankan pesan teks khususnya prosedur yang dilakukan pada kegiatan penyandian dan pengembalian teks ke bentuk semula. Sebagai input yang dibutuhkan oleh sistem adalah teks yang diinput langsung oleh *user* dapat diinputkan merupakan karakter-karakter *ASCII* 255. Berdasarkan analisa yang dilakukan terhadap data teks, maka data teks hanya disimpan dalam bentuk teks saja tidak aman sehingga siapapun masih bisa membaca dan mengerti isinya. Salah satu teknik yang umum digunakan dalam mengamankan data adalah melakukan penyandian terhadap teks dari data-data tersebut, sehingga teks-teks asli tersebut tidak dapat dimengerti oleh orang lain kecuali dilakukan proses pengembalian ke bentuk pesan asli. Ada beberapa algoritma yang dapat digunakan dalam menyandikan teks salah satunya adalah algoritma *Cipher Block Chaining* (CBC).

3.2 Penerapan Algoritma Cipher Block Chaining

Cipher Block Chaining bekerja dengan mode *block* yaitu melakukan pengelompokan biner-biner plainteks menjadi beberapa kelompok sesuai dengan ketentuan yang ditetapkan oleh pengguna (orang yang mengenkripsikan pesan). Proses enkripsi maupun dekripsi dilakukan dengan meng-XOR-kan setiap nilai blok dengan blok sebelumnya kemudian hasil yang didapatkan dari operasi XOR di XOR kan kembali dengan kunci. Biner hasil operasi XOR pada setiap blok akan digeser keposisi kiri atau kanan dengan jumlah yang ditentukan oleh pengguna sistem. Nilai awal dan kunci ditetapkan sebelum proses enkripsi maupun dekripsi dilakukan dan harus sepakati oleh pelaku enkripsi dan pelaku dekripsi. Panjang kunci dan nilai awal (*initial vector/C₀*) harus sama dengan jumlah *bit* perkelompok. Artinya apabila jumlah *bit* perkelompok sama dengan 8 *bit*, maka jumlah bit kuncidan *C₀* adalah 8 *bit*.

3.2.1 Prosedur Penerapan Cipher Blok Chaining

Adapun langkah-langkah dalam penyelesaian proses algoritma *Cipher Block Chaining* (CBC) adalah sebagai berikut:

1. Input plainteks atau cipherteks, kemudian konversikan nilai decimal kemudian kebiner
2. Tentukan nilai jumlah bit setiap kelompok, kunci, *initialization vector* (*C₀*)
3. Kelompokkan biner-biner *plaintext* dan *ciphertext* kedalam blok sesuai dengan jumlah *bit* per kelompok yang telah ditentukan sebelumnya.
4. Melakukan proses enkripsi atau dekripsi pada setiap blok/kelompok biner plaintek satau ciphertext dimana setiap blok saling ketergantungan dengan blok yang lain.
5. Lakukan proses pergeseran bit plainteks maupun cipherteks sesuai dengan jumlah bit yang ditetapkan oleh pengguna, hasil pergeseran inilah yang menjadi hasil akhir dari proses enkripsi atau dekripsi.

3.2.2 Penerapan Cipher Block Chaining untuk Proses Enkripsi

Proses enkripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $C_i = E_k (P_i \oplus C_{i-1})$. Pada pembahasan ini penulis menggunakan plaintexts= STMIK_BUDIDARMA. yang akan disandikan menjadi ciphertexts. Plainteks tersebut dirubah dahulu kedesimal dan hasilnya sebagai berikut:

1. Plaintext
Plaintext = STMIK_BUDIDARMA.

Tabel 1 : Konversi Teks To Desimal Dan Biner

Plaintext	Desimal	Biner
S	83	01010011
T	84	01010100
M	77	01001101
I	73	01001001
K	75	01001011
_	95	01011111
B	66	01000010
U	85	01010101

Plaintext	Desimal	Biner
D	68	01000100
I	73	01001001
D	68	01000100
A	65	01000001
R	82	01010010
M	78	01001101
A	65	01000001
.	46	00101110

Berikutnya kunci terlebih dahulu dan dirubah kedalam decimal setelah itu dirubah kedalam bentuk biner.

Kunci = XY (16 bit)

Plaintext	Desimal	Biner
X	88	01011000
Y	89	01011001

Berikutnya penentuan inisial vector atau C_0 , dalam penentuan bisa C_0 ditentukan sendiri

$IV/C_0 = AB$ (16 bit)

IV/C_0	Desimal	Biner
A	65	01000001
B	70	01000010

Tabel 2 Pengelompokkan Plainteks

Plaintext	Desimal	Biner
S T	83 84	01010011 01010100
M I	77 73	01001101 01001001
B U	66 85	01000010 01010101
D I	68 73	01000100 01001001
D A	68 65	01000100 01000001
R M	82 77	01010010 01001101
A .	65 46	01000001 00101110

Pengelompokkan Kunci

Kunci	Desimal	Biner
XY	88 89	01010011 01011001

Pengelompokkan IV/C₀

IV/C ₀	Desimal	Biner
A B	65 66	01000001 01000010

2. Lakukan proses enkripsi dan Dekripsi

Adapun susunan dari algoritma *CipherBlockChaining* (CBC) dalam proses enkripsi adalah sebagai berikut :

$$C_i = E_k (P_i \oplus C_{i-1})$$

$$\begin{aligned} CP_1 &= \text{Blok P1} \oplus \text{IV/C0} \\ &= 01010011 \ 01010100 \\ &= \underline{01000001 \ 01000010} \oplus \\ &= 00010010 \ 00010110 \\ &= \underline{01011000 \ 01011001} \oplus \\ &= \mathbf{01001010 \ 01001111} \end{aligned}$$

Geser empat *bit* ke kiri: 1010 0100 1111**0100** → **0100**

$$\begin{aligned} CP_2 &= \text{Blok P2} \oplus CP_1 \\ &= 01001101 \ 01001001 \\ &= \underline{1010 \ 0100 \ 11110100} \oplus \\ &= 11101001 \ 10111101 \\ &= \underline{01011000 \ 01011001} \oplus \\ &= \mathbf{10110001 \ 11100100} \end{aligned}$$

Geser empat *bit* ke kiri 00011110 0100**1011** → **1110**

$$\begin{aligned} CP_3 &= \text{Blok P3} \oplus CP_2 \\ &= 01001011 \ 01011111 \\ &= \underline{00011110 \ 01001011} \oplus \\ &= 01010101 \ 00010100 \\ &= \underline{01011000 \ 01011001} \oplus \\ &= \mathbf{00001101 \ 01001101} \end{aligned}$$

Geser empat *bit* ke kiri: 11010100 1101**0000** → **1101**

$$\begin{aligned} CP_4 &= \text{Blok P4} \oplus CP_3 \\ &= 01000010 \ 01010101 \\ &= \underline{11010100 \ 11010000} \oplus \\ &= 10010110 \ 10000101 \\ &= \underline{01011000 \ 01011001} \oplus \\ &= \mathbf{11001110 \ 11011100} \end{aligned}$$

Geser empat *bit* ke kiri: 11101101 1100**1100** → **1100**

$$\begin{aligned} CP_5 &= \text{Blok P5} \oplus CP_4 \\ &= 01000100 \ 01001001 \\ &= \underline{11101101 \ 11001100} \oplus \\ &= 10101001 \ 10010101 \\ &= \underline{01011000 \ 01011001} \oplus \\ &= \mathbf{11110001 \ 11001100} \end{aligned}$$

Geser empat *bit* ke kiri: 00011101 1100**1111** → **1100**

$$\begin{aligned} CP_6 &= \text{Blok P6} \oplus CP_5 \\ &= 01000100 \ 01000001 \\ &= \underline{00011101 \ 11001111} \oplus \end{aligned}$$

$$\begin{aligned}
 &= 01011001 \ 10001110 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= \mathbf{00000001 \ 11010111}
 \end{aligned}$$

Geser empat *bit* ke kiri: 00011101 01110000 → $\hat{I} \hat{S} \hat{S} \hat{I} \hat{P}$

$$\begin{aligned}
 CP_7 &= \text{Blok P7} \oplus \square \square C7-1 \\
 &= 01010010 \ 01001101 \\
 &= \underline{00011101 \ 01110000} \oplus \\
 &= 01001111 \ 00111101 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= \mathbf{00010111 \ 01100100}
 \end{aligned}$$

Geser empat *bit* ke kiri: 01110110 01000001 → $\hat{V} \hat{A}$

$$\begin{aligned}
 CP_8 &= \text{Blok P8} \oplus \square \square C8-1 \\
 &= 01000001 \ 00101110 \\
 &= \underline{01110110 \ 01000001} \oplus \\
 &= 00110111 \ 01101111 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= \mathbf{01101111 \ 00110110}
 \end{aligned}$$

Geser empat *bit* ke kiri: 11110011 01100110 → $\hat{O} \hat{F}$

Hasil Dekripsinya adalah: $\hat{\alpha} \hat{O} \hat{I} \hat{K} \hat{O} \hat{D} \hat{I} \hat{I} \hat{S} \hat{S} \hat{I} \hat{P} \hat{V} \hat{A} \hat{O} \hat{F}$

$$\begin{aligned}
 \hat{\alpha} &= 10100100 & \hat{O} &= 11110100 & &= 00011110 \\
 \hat{K} &= 01001011 & \hat{O} &= 11010100 & & \hat{D} = 11010000 \\
 \hat{I} &= 11101101 & \hat{I} &= 11001100 & \hat{I} \hat{S} \hat{S} &= 00011101 \\
 \hat{I} &= 11001111 & \hat{I} \hat{S} \hat{S} &= 00011101 & \hat{P} &= 01110000 \\
 \hat{V} &= 01110110 & \hat{A} &= 01000001 & \hat{O} &= 11110011 \\
 \hat{F} &= 01100110 & & & &
 \end{aligned}$$

3.2.3 Penerapan Cipher Block Chaining Untuk Proses Dekripsi

Proses Dekripsi pada *Cipher Block Chaining* (CBC) dinyatakan dengan rumus $P_i = D_k(C_i) \oplus C_{i-1}$ sebelum melakukan dekripsi chipperteks menjadi plainteks terlebih dahulu menggeser 4 bit cipherteks dari kanan. Adapun proses dekripsinya sebagai berikut :

$$C_i = D_k (P_i \oplus C_{i-1})$$

$$C_0 = 01000001 \ 01000010$$

$$C_1 = 1010 \ 0100 \ 1111\mathbf{0100} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{0100}1010 \ 01001111$$

$$C_2 = 00011110 \ 0100\mathbf{1011} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{1011}0001 \ 11100100$$

$$C_3 = 11010100 \ 1101\mathbf{0000} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{0000}1101 \ 01001101$$

$$C_4 = 11101101 \ 1100\mathbf{1100} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{1100}1110 \ 11011100$$

$$C_5 = 00011101 \ 1100\mathbf{1111} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{1111}0001 \ 11001100$$

$$C_6 = 00011101 \ 0111\mathbf{0000} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{0000}0001 \ 11010111$$

$$C_7 = 01110110 \ 0100\mathbf{0001} \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{0001}0111 \ 01100100$$

$$C_8 = 11110011 \ 01100110 \rightarrow \text{Geser empat } bit \text{ ke kanan } \mathbf{0110}1111 \ 00110110$$

$$\begin{aligned}
 P1 &= C1 \oplus C0 \\
 &= 01001010 \ 01001111 \\
 &= \underline{01000001 \ 01000010} \oplus \\
 &= 00001011 \ 00001101 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= 01010011 \ 01010100 \rightarrow \mathbf{ST}
 \end{aligned}$$

$$\begin{aligned}
 P2 &= C2 \oplus C2-1 \\
 &= 10110001 \ 11100100 \\
 &= \underline{1010 \ 0100 \ 11110100} \oplus \\
 &= 00010101 \ 00010000
 \end{aligned}$$

$$\begin{aligned}
 &= \underline{01011000 \ 01011001} \oplus \\
 &= 01001101 \ 01001001 \rightarrow \mathbf{MI} \\
 &\dots \\
 P7 &= C7 \oplus C7-1 \\
 &= 00010111 \ 01100100 \\
 &= \underline{00011101 \ 01110000} \oplus \\
 &= 00001010 \ 00010100 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= 01010010 \ 01001101 \rightarrow \mathbf{RM} \\
 P8 &= C8 \oplus C8-1 \\
 &= 01101111 \ 00110110 \\
 &= \underline{01110110 \ 01000001} \oplus \\
 &= 00011001 \ 01110111 \\
 &= \underline{01011000 \ 01011001} \oplus \\
 &= 01000001 \ 00101110 \rightarrow \mathbf{A}.
 \end{aligned}$$

Jadi, hasil dekripsi adalah :**STMIK_BUDIDARMA.**

S=00101001 T=01010100 M=01001101 I=01001001 K=01001011 _=01011111
B=01000010 U=01010101 D=01000100 I=01001001 D=01000100 A=01000001
R=01010010 M=01001101 A=01000001 .=00101110

3.3. Implementasi

Pengujian yang dilakukan adalah pengujian metode (*MethodTesting*) terhadap hasil manual yang sudah dikerjakan sebelumnya pada bab 3 dengan menggunakan program yang sudah dibuat.

Implementasi program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*Software*).

From Enkripsi berfungsi untuk melakukan proses enkripsi dimana *user* harus menginput teks yang akan di enkripsi. Berikut Tampilan enkripsi



Gambar 3 Tampilan Form Enkripsi

From Dekripsi berfungsi untuk melakukan proses dekripsi, dimana *user* harus menginput teks yang akan di dekripsi. Berikut tampilan Form Dekripsi



Gambar 4 Gambar Form Tampilan Dekripsi

4. KESIMPULAN

Berdasarkan hasil dari penelitian yang penulis lakukan mengenai Perancangan Aplikasi Penyandian Teks Dengan Menggunakan Algoritma Chipher Block Chaining maka penulis dapat menarik kesimpulan sebagai berikut:

1. Proses penyandian teks dengan menggunakan algoritma *CipherBlockChaining* (CBC) dilakukan dengan merubah dahulu teks asli dalam bentuk desimal untuk seterusnya konversikan ke biner kemudian melakukan *InisialVector*
2. Proses enkripsi dengan algoritma *CipherBlockChaining* (CBC) dilakukan dengan teks asli yang sudah konversikan ke biner sebelumnya di kelompokkan beberapa blok seterusnya di XOR kan ke kunci yang sudah ditentukan, setelah itu hasil XOR tersebut digeser 4 *bit* dari kiri kekanan. Proses Dekripsi dengan algoritma *CipherBlockChaining* (CBC) dilakukan dengan teks asli yang sudah di enkrip di geser dahulu dari kanan ke kiri sebanyak 4 *bit* setelah itu di- XOR- kan dengan *InisialVector*.
3. Untuk merancang aplikasi penyandian teks menggunakan algoritma *CipherBlockChaining* (CBC) dilakukan dengan merancang *usecase diagram*, *activity diagram* dan *Microsoft Visualstudio 2008* untuk rancangan *interface* enkripsi dan dekripsi yang nantinya digunakan sebagai pengujian bagi *user*.

DAFTAR PUSTAKA

- [1] Antonius Rachmat C (2010), Algoritma dan Pemrograman dengan Bahasa C- Konsep, Teori, & Implementasi, Yogyakarta: Andi
- [2] A.S Rosa, Salahuddin, M (2011), Modul Pembelajaran Rekayasa Perangkat Lunak(Terstruktur dan Berorientasi Objek).
- [3] Dewi Rosmala (2012), Implementasi Mode Cipher Block Chaining (CBC) pada pengamanan Data, Vol.3, 2012
- [4] Doni Ariyus (2006), Kriptografi Keamanan Data dan Komunikasi, Yogyakarta: Andi
- [5] [http //id.wikipedia org/wiki/ASCII](http://id.wikipedia.org/wiki/ASCII). (Tanggal akses 07 juni 2015)
- [6] [http //id.wikipedia org/wiki/Perancangan](http://id.wikipedia.org/wiki/Perancangan).(Tanggal akses 04 Agustus 2015)
- [7] [http //id.wikipedia org/wiki/Aplikasi](http://id.wikipedia.org/wiki/Aplikasi).(Tanggal akses 04 Agustus 2015)
- [8] Rifki Sadikin, (2012), Kriptografi Keamanan Data, Yogyakarta, Andi
- [9] Rinaldi Munir (2006), Kriptografi, Informatika, Bandung
- [10] Taronisoki Zebua (2013), Analisa dan Penyandian Algoritma Triangle Chain Pada Penyandian Record Database, Pelita Informatika Budidarma, Vol.III, 2301-9425
- [11] Wahana Komputer (2009), Membangun Aplikasi Toko Dengan Visual Basic 2008, Yogyakarta, Andi