PERBANDINGAN MODE CHIPER ELECTRONIC CODE BOOK DAN CHIPER BLOCK CHAINING DALAM PENGAMANAN DATA

Arif Kurnia Rachman
Program Studi Teknik Informatika
Jurusan Teknik Elektro Universitas Diponegoro
E-mail : thegreatsolomon@gmail.com

ABSTRACT

Cryptographic algorithm has undergone rapid development as an effort of securing data.Block Chiper is one of the cryptographic algorithms that have proven to be secure data important data in the field of informatika.The one type of block cipher cryptographic algorithm is ECB (Electronic Code Book) and CBC (chiper Block chaining)

Both modes this block has been trusted to secure data in the field of cryptograph. In ECB mode, ie each block of the same plaintext will always be encrypted into the same blocks ciphertext. the ECB appears from the fact that since the same plaintext block always encrypted into the same blocks ciphertext, while the CBC mode block ciphertext depends not only on the block plaintext. but also on all previous plaintext blocks.

Keyword : Cryptographic, block cipher, ECB mode, CBC mode

INTISARI

Algoritma kriptografi telah mengalami perkembangan pesat sebagai upaya dari pengamanan data.Blok Chiper adalah salah satu algoritma kriptografi yang telah terbukti dapat mengamankan data data penting dalam bidang informatika.Salah satu jenis algoritma kriptografi blok cipher adalah ECB (Electronic Code Book) dan CBC (chiper Block Chaining)

Kedua mode blok ini telah dipercaya untuk mengamankan data dalam bidang kriptografi. dalam mode ECB, yaitu setiap blok plainteks yang sama akan selalu dienkripsi menjadi blok chiperteks yang sama. dalam ECB muncul dari fakta bahwa karena blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama, sedangkan mode CBC blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.

Kata kunci : Kriptografi, blok chiper,mode ECB, mode CBC

PENDAHULUAN

Dalam masalah keamanan data, ilmu kriptografi sangat penting untuk dikembangkan dan di terapkan.setiap data haruslah dienkripsi dan dapat didekripsi denagn baik sehingga keamanan data lebih terjamin.

Blok Cipher pada kriptografi dalam perkembangannya dikelompokkan menjadi beberapa jenis mode yang dapat menyimpan data dengan melalui proses matematik dan penyandian terstruktur serta pembagian ke dalam sub bagian blok blok tertentu dalam suatu bit biner (Brumley 2010).

Pada cipher blok, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama, biasanya 64 bit (tapi adakalanya lebih). Algoritma enkripsi menghasilkan blok cipherteks yang pada kebanyakan sistem kriptografi simetri berukuran sama dengan blok plainteks

Dengan blok cipher, blok plainteks yang sama akan dienkripsi menjadi blok cipherteks yang sama bila digunakan kunci yang sama pula. Ini berbeda dengan cipher aliran dimana bit-bit plainteks yang sama akan dienkripsi menjadi bit-bit cipherteks yang berbeda setiap kali dienkripsi.

Dalam makalah ini akan diperbandingkan algoritma kriptografi blok cipher antara mode ECB dan CBC berikut tentang kelemahan dan keunggulan masing masing algoritma tersebut.

LATAR BELAKANG

Penerapan suatu blok cipher membutuhkan proses yang panjang dalam penyandiannya.Penyandiannya sendiri baik mode ECB maupun CBC memiliki struktur blok yang terbagi bagi kedalam sub sub bagian, dimana tiap bagian memiliki proses dan algoritma penyelesaianan tersendiri berdasarkan bit bit pesan yang akan di enkripsi (Thomas,2006)

Bit bit pesan yang akan dienkripsi biasanya terdiri dari 64 bit ,dengan demikian pada blok cipher bit tersebut terbagi menjadi beberapa bagian yang dilanjutkan dengan proses algoritma sesuai alur yang ada pada blok cipher. (Schneier,1994)

Algoritma blok cipher tersebut menggabungkan beberapa teknik kriptografi modern dalam proses enkripsi. Dengan kata lain, cipher blok dapat diacu sebagai super-enkripsi.

Teknik kriptografi modern yang digunakan adalah:

a. Substitusi.

Teknik ini mengganti satu atau sekumpulan bit pada blok plainteks tanpa mengubah urutannya. Secara matematis, teknik substitusi ini ditulis sebagai

$$c_i = E(p_i),\ i = 1, 2, \ldots \text{ (urutan bit)} \qquad (1)$$

yang dalam hal ini c_i adalah bit cipherteks, p_i adalah bit plainteks, dan f adalah fungsi substitusi. Dalam praktek, E dinyatakan sebagai fungsi matematis atau dapat merupakan tabel susbtitusi (S-box).

b. Transposisi atau permutasi

Teknik ini memindahkan posisi bit pada blok plainteks berdasarkan aturan tertentu. Secara matematis, teknik transposisi ini ditulis sebagai

$$C = PM \qquad (2)$$

yang dalam hal ini C adalah blok cipherteks, P adalah blok plainteks, dan M adalah fungsi transposisi. Dalam praktek, M dinyatakan sebagai tabel atau matriks permutasi.

c. Ekspansi

Teknik ini memperbanyak jumlah bit pada blok plainteks berdasarkan aturan tertentu, misalnya dari 32 bit menjadi 48 bit. Dalam praktek, aturan eskpansi dinyatakan dengan tabel.

d. Kompresi

Teknik ini kebalikan dari ekspansi, di mana jumlah bit pada blok plainteks diciutkan berdasarkan aturan tertentu. Dalam praktek, aturan kompresi dinyatakan dengan table (Lubbe.2004)

Keempat teknik ini digunakan secara bersama sama untuk melakukan penyandian data pada blok cipher.

Dasar Teori

Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter (seperti yang dilakukan pada chiper subtitusi atau chiper transposisi dari algoritma kriptografi modern) (Brumley 2010).

Operasi dalam mode bit berarti semua data dan informasi, baik kunci, plainteks, ataupun chiperteks, dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memroses semua data dan informasi dalam rangkaian bit. Rangkaian bit yang menyatakan plainteks dienkripsi menjadi chiperteks dalam bentuk rangkaian bit, demikian sebaliknya.

Blok Chiper

Dalam proses enkripsi atau dekripsi yang memiliki kunci simetri (Algoritma kunci simetri yang merupakan salah satu kategori dari algoritma kriptografi modern mengacu pada metode enkripsi yang dalam hal ini baik pengirim maupun penerima memiliki kunci yang sama.), pemrosesan dapat dilakukan dengan dua metode, Cipher aliran (stream cipher) dan Cipher blok (block cipher).

Pada metode cipher blok, proses enkripsi maupun dekripsi dilakukan terhadap sekelompok blok yang terdiri dari sejumlah bit. Panjang bit sudah diketahui sebelumnya dan disesuaikan dengan panjang kunci, biasanya 64 bit atau lebih.

Algoritma enkripsi menghasilkan blok cipherteks yang berukuran sama dengan blok plainteks .

Dekripsi dilakukan dengan cara yang serupa seperti enkripsi.

Misalkan blok plainteks (P) yang berukuran m bit dinyatakan sebagai vektor

$$P = (p1, p2, ..., pm) \qquad (3)$$

yang dalam hal ini pi adalah bit 0 atau bit 1 untuk i = 1, 2, …, m, dan blok cipherteks (C) adalah

$$C = (c1, c2, ..., cm) \qquad (4)$$

yang dalam hal ini ci adalah bit 0 atau bit 1 untuk i = 1, 2, …, m.

Bila plainteks dibagi menjadi n buah blok, barisan blok-blok plainteks dinyatakan sebagai

$$(P1, P2, \ldots, Pn) \qquad (5)$$

Untuk setiap blok plainteks Pi, bit-bit penyusunnya dapat dinyatakan sebagai vektor

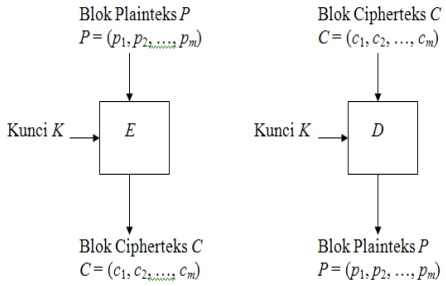
$$Pi = (pi1, pi2, ..., pim) \qquad (6)$$

Enkripsi dengan kunci K dinyatakan dengan persamaan

$$Ek(P) = C \quad (7)$$

sedangkan dekripsi dengan kunci K dinyatakan dengan persamaan

$$Dk(C) = P \quad (8)$$



Gambar 1 Blok Chiper

Perbandingan Mode ECB dan CBC
Mode Electronic Code Book (ECB)

Enkripsi dan dekripsi yang sifatnya acak ini sangat cocok diimplementasikan dengan algoritma block chiper mode ECB (Electronic Code Book), dengan syarat setiap record terdiri dari sejumlah blok diskrit yang sama banyaknya. Mode ECB cocok untuk mengenkripsi file yang diakses secara acak karena tiap blok plaintext dienkripsi secara independen. Bahkan jika mode ECB dikerjakan dengan prosesor paralel, maka setiap prosesor dapat melakukan enkripsi atau dekripsi blok plainteks yang berbeda-beda (Rijmen. 1999)

ECB yang akan digunakan untuk mengenkripsi atau mendekripsi data adalah ECB yang telah dimodifikasi agar blok chiperteks yang dihasilkan tidak sama meskipun mengenkripsi plainteks yang sama. Hal ini untuk menghindari bagian plainteks yang sering berulang, yang menjadi salah satu kelemahan mode ECB.

Pada mode ini, setiap blok plainteks dienkripsi secara individual dan independen. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai

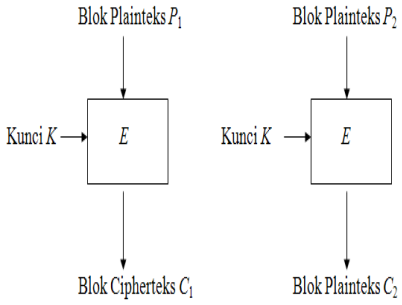
$$C_i = E_K(P_i) \quad (9)$$

dan dekripsi sebagai

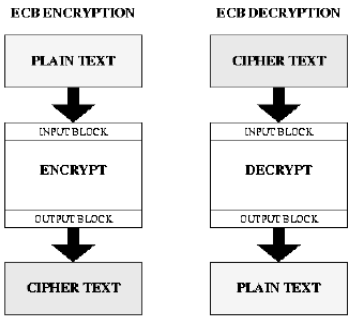
$$P_i = D_K(C_i) \quad (10)$$

yang dalam hal ini, P_i dan C_i masing-masing blok plainteks dan cipherteks ke-i.

Gambar 2 memperlihatkan enkripsi dua buah blok plainteks, P_1 dan P_2 dengan mode ECB, yang dalam hal ini E menyatakan fungsi enkripsi yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci K.



Gambar 2. Skema enkripsi dan dekripsi dengan mode *ECB*



Gambar 3 Blok chiper mode ECB

Misalkan plainteks (dalam biner) adalah

10100010001110101001

Bagi plainteks menjadi blok-blok yang berukuran 4 bit:

1010 0010 0011 1010 1001

atau dalam notasi HEX adalah A23A9.

Misalkan kunci (K) yang digunakan adalah (panjangnya juga 4 bit)

1011

atau dalam notasi HEX adalah B.

Misalkan fungsi enkripsi E yang sederhana (tetapi lemah) adalah dengan meng-XOR-kan blok plainteks P_i dengan K, kemudian geser secara wrapping bit-bit dari

$P_i \oplus K$ satu posisi ke kiri.

Proses enkripsi untuk setiap blok digambarkan sebagai berikut:

1010 0010 0011 1010 1001
1011 1011 1011 1011 1011
⊕
XOR: 0001 1001 1000 0001 0010
Geser: 0010 0011 0001 0010 0100
Dalam notasi HEX: 23124

Jadi, hasil enkripsi plainteks

1010001000111010100 1
(A23A9 dalam notasi HEX)

adalah

00100011000100100100 (23124 dalam notasi HEX)

Catatlah bahwa blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama (atau identik). Pada contoh 1 di atas, blok 1010 muncul dua kali dan selalu dienkripsi menjadi 0010.

Kata "code book" di dalam ECB muncul dari fakta bahwa karena blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama, maka secara teoritis dimungkinkan membuat buku kode plainteks dan cipherteks yang berkoresponden (Rijmen. 1999)

Namun, semakin besar ukuran blok, semakin besar pula ukuran buku kodenya. Misalkan jika blok berukuran 64 bit, maka buku kode terdiri dari $2^{64} - 1$ buah kode (entry), yang berarti terlalu besar untuk disimpan. Lagipula, setiap kunci mempunyai buku kode yang berbeda.

Padding

Ada kemungkinan panjang plainteks tidak habis dibagi dengan panjang ukuran blok yang ditetapkan (misalnya 64 bit atau lainnya). Hal ini mengakibatkan blok terakhir berukuran lebih pendek daripada blok-blok lainnya. (Lubbe.2004)

Satu cara untuk mengatasi hal ini adalah dengan padding, yaitu menambahkan blok terakhir dengan pola bit yang teratur agar panjangnya sama dengan ukuran blok yang ditetapkan. Misalnya ditambahkan bit 0 semua, atau bit 1 semua, atau bit 0 dan bit 1 berselang-seling.

Misalkan ukuran blok adalah 64 bit (8 byte) dan blok terakhir terdiri dari 24 bit (3 byte). Tambahkan blok terakhir dengan 40 bit (5 byte) agar menjadi 64 bit, misalnya dengan menambahkan 4 buah byte 0 dan satu buah byte angka 5. Setelah dekripsi, hapus 5 byte terakhir dari blok dekripsi terakhir.

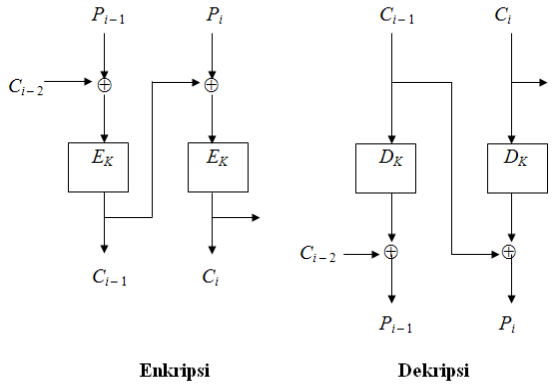
Mode Cipher Block Chaining (CBC)

Mode ini menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*.

Caranya, blok plainteks yang *current* di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi.

Dengan mode *CBC*, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.

Dekripsi dilakukan dengan memasukkan blok cipherteks yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Dalam hal ini, blok cipherteks sebelumnya berfungsi sebagai umpan-maju (*feedforward*) pada akhir proses dekripsi. Gambar 5 memperlihatkan skema mode operasi *CBC*.



Gambar 5 Skema enkripsi dan dekripsi dengan mode *CBC*

Secara matematis, enkripsi dengan mode *CBC* dinyatakan sebagai

$$C_i = E_K(P_i \oplus C_{i-1}) \qquad (11)$$

dan dekripsi sebagai

$$P_i = D_K(C_i) \oplus C_{i-1} \qquad (12)$$

Blok plainteks pertama menggunakan C_0 sebagai vektor awal (*initialization vector* atau IV). IV tidak perlu rahasia.Blok-blok plainteks yang identik

dienkripsi menjadi blok-blok cipherteks yang berbeda hanya jika blok-blok plainteksnya sebelumnya berbeda.

Jika blok-blok plainteks sebelumnya ada yang sama, maka ada kemungkinan cipherteksnya sama. Untuk mencegah hal ini, maka digunakan IV yang merupakan data acak sebagai blok pertama. IV tidak mempunyai makna, ia hanya diguanakan untuk membuat tiap blok cipherteks menjadi unik.

Tinjau kembali painteks (dalam biner) pada pesan sebelumnya didapat

10100010001110101001

Bagi plainteks menjadi blok-blok yang berukuran 4 bit:

1010 0010 0011 1010 1001

atau dalam notasi HEX adalah A23A9.

Misalkan kunci (*K*) yang digunakan adalah (panjangnya juga 4 bit)

1011

atau dalam notasi HEX adalah B. Sedangkan IV yang digunakan seluruhnya bit 0 (Jadi, C_0 = 0000)

Misalkan fungsi enkripsi *E* yang sederhana (tetapi lemah) adalah dengan meng-XOR-kan blok plainteks P_i dengan *K*, kemudian geser secara *wrapping* bit-bit dari $P_i \oplus K$ satu posisi ke kiri.

C_1 diperoleh sebagai berikut:

$$P_1 \oplus C_0 = 1010 \oplus 0000 = 1010$$

Enkripsikan hasil ini dengan fungsi *E* sbb:

$$1010 \oplus K = 1010 \oplus 1011 = 0001$$

Geser (*wrapping*) hasil ini satu bit ke kiri: 0010

Jadi, C_1 = 0010 (atau 2 dalam HEX)

C_2 diperoleh sebagai berikut:
$P_2 \oplus C_1 = 0010 \oplus 0010 = 0000$
$0000 \oplus K = 0000 \oplus 1011 = 1011$
Geser (*wrapping*) hasil ini satu bit ke kiri: 0111

Jadi, C_2 = 0111 (atau 7 dalam HEX)

C_3 diperoleh sebagai berikut:
$P_3 \oplus C_2 = 0011 \oplus 0111 = 0100$
$0100 \oplus K = 0100 \oplus 1011 = 1111$
Geser (*wrapping*) hasil ini satu bit ke kiri: 1111
Jadi, C_2 = 1111 (atau F dalam HEX)

Demikian seterusnya, sehingga plainteks dan cipherteks hasilnya adalah:

Pesan (plainteks): A23A9
Cipherteks (mode *ECB*): 23124
Cipherteks (mode *CBC*): 27FBF

Terlihat bahwa dengan menggunakan mode *CBC*, blok plainteks yang sama (A dalam HEX) dienkripsikan menjadi dua blok cipherteks yang berbeda (masing-masing 2 dan B). Bandingkan dengan mode *EBC* yang menghasilkan blok cipherteks yang sama (2 dalam HEX) untuk dua buah blok yang sama (A).

Dengan kata lain, pada mode *CBC*, tidak ada korelasi antara posisi blok plainteks yang sams dengan posisi blok cipherteksnya

Kelemahan dan kelebihan Mode ECB dan CBC
Kelemahan dan kelebihan Mode ECB
Kelebihan Mode ECB

Karena tiap blok plainteks dienkripsi secara independen, maka kita tidak perlu mengenkripsi file secara linear. Kita dapat mengenkripsi 5 blok pertama, kemudian blok-blok di akhir, dan kembali ke blok-blok di tengah dan seterusnya.
Mode *ECB* cocok untuk mengenkripsi arsip (*file*) yang diakses secara acak, misalnya arsip-arsip basis data. Jika basisdata dienkripsi dengan mode *ECB*, maka sembarang *record* dapat dienkripsi atau didekripsi secara independen dari *record* lainnya (dengan asumsi setiap *record* terdiri dari sejumlah blok diskrit yang sama banyaknya)
(Brumley 2010).

Jika mode *ECB* dikerjakan dengan prosesor paralel (*multiple processor*), maka setiap prosesor dapat melakukan enkripsi atau dekripsi blok plainteks yang berbeda-beda.

Jika satu atau lebih bit pada blok cipherteks mengalami kesalahan, maka kesalahan ini hanya mempengaruhi cipherteks yang bersangkutan pada waktu dekripsi. Blok-blok cipherteks lainnya bila

didekripsi tidak terpengaruh oleh kesalahan bit cipherteks tersebut.

Kelemahan ECB

Karena bagian plainteks sering berulang (sehingga terdapat blok-blok plainteks yang sama), maka hasil enkripsinya menghasilkan blok cipherteks yang sama (lihat Contoh 1).

Bagian plainteks yang sering berulang misalnya kata-kata seperti (dalam Bahasa Indonesia) *dan*, *yang*, *ini*, *itu*, dan sebagainya.

Di dalam *e-mail*, pesan sering mengandung bagian yang redundan seperti *string* 0 atau spasi yang panjang, yang bila dienkripsi maka akan menghasilkan pola-pola cipherteks yang mudah dipecahkan dengan serangan yang berbasis statistik (menggunakan frekuensi kemunculan blok cipherteks). Selain itu, *e-mail* mempunyai struktur yang teratur yang menimbulkan pola-pola yang khas dalam cipherteksnya.

Kelemahan dan kelebihan Mode CBC
Keuntungan CBC

Pesan menjadi jauh lebih aman untuk dideteksi kuncinya karena kunci tiap blok berbeda beda tergantung dari plaintext sebelumnya

Kelemahan CBC

Karena blok cipherteks mempengaruhi blok-blok berikutnya, pihak lawan dapat menambahkan blok cipherteks tambahan pada akhir pesan terenkripsi tanpa terdeteksi. Ini akan menghasilkan blok plainteks tambahan pada waktu dekripsi.

Pesan moral untuk masalah ini, pengirim pesan seharusnya menstrukturkan plainteksnya sehingga ia mengetahui di mana ujung pesan dan dapat mendeteksi adanya blok tambahan.

Pihak lawan dapat mengubah cipherteks, misalnya mengubah sebuah bit pada suatu blok cipherteks. Tetapi hal ini hanya mempengaruhi blok plainteks hasil dekripsinya dan satu bit kesalahan pada posisi plainteks berikutnya.

KESIMPULAN

Dari pembahasan diatas didapatkan bahwa masing masing dari mode blok chiper tersebut memiliki kelebihan dan kekurangan masing masing.Kita dapat dengan bijak menentukan algoritma kriptografi yang tepatuntuk menyandikan pesan kita, mode ECB meneyediakan algoritma yang lebih sederhana denga kemampuan dekripsi dan enkripsi yang tepat dan tepat tetapi memiliki kelemahan jika nilai kuncinya diketaui maka pesan tersebut dapat terbongkar.

Sedangkan pada mode CBC prosesnya jauh lebih rumit dan membutuhkan penanganan matematik lebih dari mode ECB namun demikian keamanan data dapat tersimpan lebih rahasia karena bit bit yang etrenkripsi bukandari plain text langsung melainkan dari bit bit yang telah terenkripsi sebelumnya.

Kedua mode tersebut menjadi beberapa pilihan dari algoritma kriptografi modern yang telah dikembangkan bertahun tahun.sebagai algoritma penyandian data kedua mode blok chiper tersebut menjadi suatu pilihan yang menarik untuk penyandian data.

DAFTAR PUSTAKA

Billy Bob Brumley and Kimmo U. Ja¨ rvinen.2010" Conversion Algorithms and Implementations for Koblitz Curve Cryptography".IEEE TRANS. ON DEPENDABLE AND SECURE COMPUTING,

V. Rijmen. 1999."Chipper Block".

K.Cartrysse and J.C.A. van der Lubbe.1994 "Basic methods of cryptography"

B.Schneier, Applied Cryptography, John Wiley & Sons, New York,

Baigneres,Thomas and Serge Vaudenay ,2006 "*AClassical Introduction to Cryptography: Exercise Book*"

http://infokriptografi.com

www.ilmu-komputer.net