Studi dan Implementasi Pengamanan Basis Data pada Microsoft Sql Server 2005 dengan *Block Cipher*

Mohamad Irvan Faradian
Program Studi Teknik Informatika, STEI, ITB, Bandung 40132, email: if14024@students.if.itb.ac.id

Abstrak – *Masalah keamanan data merupakan salah satu masalah yang terdapat dalam penyimpanan data-data dalam sebuah basis data. Jika data-data yang tersimpan tersebut merupakan data-data rahasia yang tidak boleh diakses oleh semua orang, data-data tersebut haruslah terjamin keamanannya. Makalah ini menguraikan penerapan pengamanan pada basis data dengan melakukan enkripsi pada data-data sebelum dimasukkan ke dalam basis data. Enkripsi tersebut dilakukan dengan menggunakan block cipher dengan algoritma yang dirancang sendiri. Mode block cipher yang digunakan ialah ECB, CBC, dan CFB. Studi yang dilakukan ialah mencari cara agar dapat mengamankan data-data dengan menggunakan block cipher dalam sebuah basis data dimana pada umumnya teknik yang digunakan untuk mengamankan data-data dalam sebuah basis data ialah dengan menggunakan stream cipher.*

Kata Kunci*: Basis Data, Kriptografi, Block Cipher, ECB, CBC, dan CFB*

1. PENDAHULUAN

Pada zaman komputer sekarang ini, mayoritas perusahaan besar telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data-data, baik data-data pegawai perusahaanya maupun data-data yang terkait kepentingan bisnis perusahaan tersebut. Untuk data-data yang sangat penting seperti data-data yang terkait dengan kepentingan bisnis perusahaan tersebut, maka dibutuhkan keamanan agar data-data tersebut tidak dapat dilihat isinya oleh orang-orang yang tidak berhak, seperti perusahaan pesaing yang juga bergerak dalam bidang yang sama maupun orang dalam perusahaan yang juga tidak berhak.

Selain mengamankan data-data pada level jaringan dimana client berkomunikasi dengan server melalui *query-query* yang dijalankan maupun pengaturan hak akses oleh administrator basis data, pengamanan dapat pula dilakukan dengan cara melakukan enkripsi terhadap data-data sebelum dimasukkan ke dalam basis data. Jika ada seorang pengguna yang ingin membaca isi dari basis data tersebut, maka pengguna tersebut harus melakukan dekripsi terhadap data-data yang tersimpan di dalam basis data dengan memasukkan kunci yang sama yang digunakan untuk melakukan enkripsi terhadap data sebelum dimasukkan ke dalam basis data.

Penerapan kriptografi pada makalah ini menggunakan *block cipher* dengan tiga mode, yaitu *Electronic Code Book (ECB), Cipher Block Chaining (CBC),* dan *Cipher Feedback (CFB)* dengan menggunakan rancangan algoritma sendiri.

2. RANCANGAN ALGORITMA

2.1. Mode operasi *block cipher*

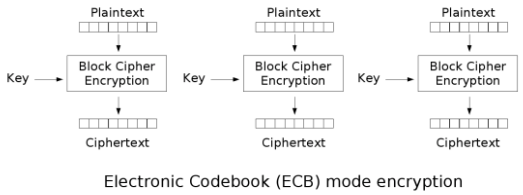
a. Mode *Electronic Code Book (ECB)*
Pada mode ini, setiap blok plainteks P_i dienkripsi secara individual dan independen menjadi blok cipherteks C_i. Secara matematis, enkripsi dengan mode *ECB* dinyatakan sebagai

$$C_i = Ek(P_i) \qquad \textit{persamaan (1)}$$

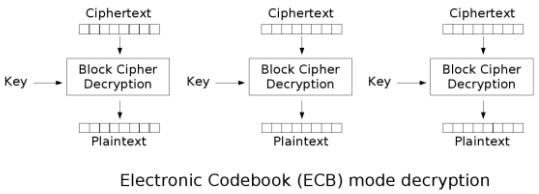
dan dekripsi sebagai

$$P_i = Dk(C_i) \qquad \textit{persamaan (2)}$$

yang dalam hal ini P_i dan C_i masing-masing blok plainteks dan cipherteks ke-i. Gambar di bawah ini memperlihatkan enkripsi blok plainteks dengan mode *ECB*, yang dalam hal ini *E* menyatakan fungsi enkripsi yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci *K*.



Gambar 1 : Enkripsi pada *ECB*



Gambar 2 : Dekripsi pada *ECB*

b. Mode *Cipher Block Chaining (CBC)*
Pada mode ini, terdapat mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dalam hal ini hasil

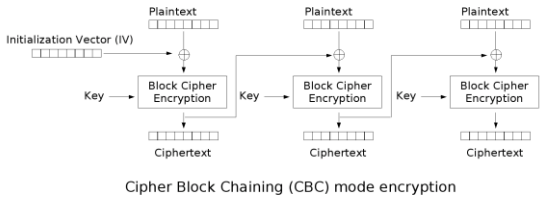
enkripsi blok sebelumnya diumpan-balikkan ke dalam enkripsi blok yang sedang diproses. Caranya, blok plainteks yang sedang diproses di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan mode *CBC*, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya. Dekripsi dilakukan dengan memasukkan blok cipherteks yang sedang diproses ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Dalam hal ini, blok cipherteks berfungsi sebagai umpan-maju (*feedforward*) pada proses dekripsi. Secara matematis, enkripsi dengan mode *CBC* dinyatakan sebagai

$$C_i = E_k(P_i + C_{i-1}) \qquad \textit{persamaan (3)}$$

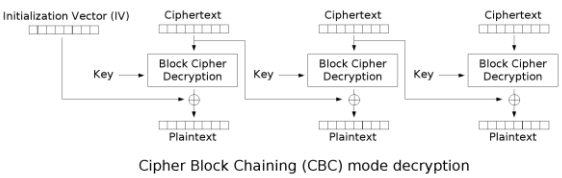
dan dekripsi sebagai

$$P_i = D_k(C_i) + C_{i-1} \qquad \textit{persamaan (4)}$$

yang dalam hal ini, $C_0 = IV$ (*Initialization Vector*). *IV* dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh program. Jadi, untuk menggantikan blok cipherteks pertama (C_1), *IV* digunakan untuk menggantikan blok cipherteks sebelumnya, C_0. Sebaliknya pada dekripsi, blok plainteks diperoleh dengan meng-XOR-kan *IV* dengan hasil dekripsi terhadap blok cipherteks pertama. Gambar di bawah ini memperlihatkan enkripsi blok plainteks dengan mode *CBC*, yang dalam hal ini *E* menyatakan fungsi enkripsi yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci *K*.



Gambar 3 : Enkripsi pada CBC



Gambar 4 : Dekripsi pada CBC

Perhatikan bahwa enkripsi terhadap blok i adalah fungsi dari semua plainteks dari blok 0 sampai blok i – 1, sehingga blok plainteks yang sama menghasilkan blok cipherteks yang berbeda hanya jika blok-blok plainteks 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 memiliki makna, ia hanya digunakan untuk meembuat tiap blok cipherteks menjadi unik.

c. Mode Cipher Feedback (CFB)

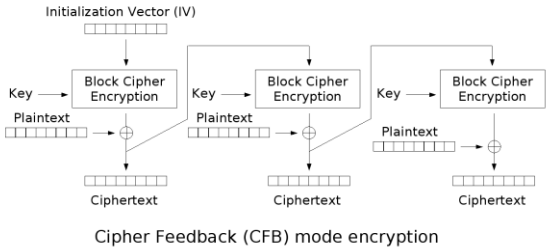
Mode ini mirip dengan mode *CBC* yang menggunakan mekanisme umpan-balik. Pada mode ini, hasil enkripsi blok sebelumnya langsung masuk ke dalam fungsi enkripsi, baru kemudian di-XOR-kan dengan blok plainteks, tidak seperti *CBC* yang di-XOR-kan terlebih dahulu dengan blok plainteks. Data yang dienkripsi dengan mode ini boleh menggunakan unit yang lebih kecil daripada ukuran blok. Unit yang dienkripsi dapat berupa bit per bit (jadi seperti cipher aliran), 2 bit, 3 bit, dan seterusnya. Jika unit yang dienkripsi satu karakter setiap kalinya, maka mode *CFB*-nya disebut *CFB* 8 bit. Namun, dalam laporan ini, panjang bit yang digunakan sesuai dengan panjang kunci, yaitu panjang kunci * 8 bit. Secara matematis, enkripsi dengan mode *CFB* dinyatakan sebagai

$$C_i = P_i + E_k(C_{i-1}) \qquad \textit{persamaan (5)}$$

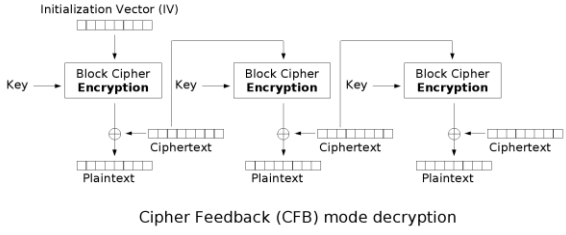
dan dekripsi sebagai

$$P_i = C_i + D_k(P_{i-1}) \qquad \textit{persamaan (6)}$$

Gambar di bawah ini memperlihatkan enkripsi blok plainteks dengan mode *CBC*, yang dalam hal ini *E* menyatakan fungsi enkripsi yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci *K*.



Gambar 5 : Enkripsi pada CFB



Gambar 6 : Dekripsi pada CFB

2.2. Algoritma enkripsi dan dekripsi

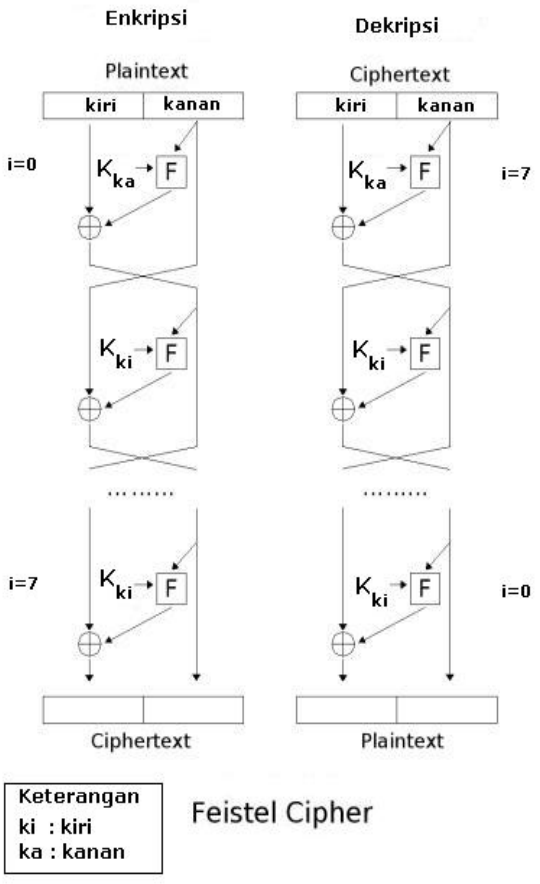
Panjang blok adalah sesuai panjang kunci. Panjang kunci di sini diharuskan kelipatan 2 dan panjangnya minimal 8 karakter. Mula-mula blok pertama masuk ke jaringan Feistel, kemudian kunci dan blok tersebut

dibagi menjadi dua bagian, blok bagian kanan dikenakan algoritma iCrypt. Berikut ini adalah alur pada algoritma iCrypt untuk proses enkripsi:

a) Blok bagian kanan dilakukan operasi pergeseran bit sejauh 3.
b) Kemudian blok bagian kanan dilakukan operasi pembalikan bit, yang bernilai 0 menjadi 1 dan yang benilai 1 menjadi 0.
c) Jika putaran genap, maka operasi XOR pada blok bagian kanan dilakukan dengan menggunakan kunci bagian kanan. Sebaliknya, operasi XOR dilakukan dengan menggunakan kunci bagian kiri.
d) Lakukan kembali operasi pada blok bagian kanan hingga sejumlah batas maksimum putaran jaringan Fiestel, dalam hal ini sebanyak 16 kali.

Sedangkan alur pada algoritma iCrypt untuk proses dekripsi:

a) Blok bagian kanan dilakukan operasi penggeseran bit sejauh 3.
b) Kemudian blok bagian kanan dilakukan operasi pembalikan bit, yang bernilai 0 menjadi 1 dan yang benilai 1 menjadi 0.
c) Jika putaran ganjil, maka operasi XOR pada blok bagian kanan dilakukan dengan menggunakan kunci bagian kanan. Sebaliknya, operasi XOR dilakukan dengan menggunakan kunci bagian kiri.
d) Lakukan kembali operasi pada blok bagian kanan. Putaran pada jaringan Fiestel dilakukan sebanyak 16 kali.



Gambar 7 : Jaringan Feistel

3. IMPLEMENTASI

Untuk melakukan studi dan penerapan pengamanan dengan menggunakan block cipher pada basis data ini, maka dibangun sebuah perangkat lunak berbasis web yang dibangun di antara server basis data dan web browser.

Gambar 8 : Deskripsi umum sistem perangkat lunak

Perangkat lunak yang dibangun menerima masukan dari pengguna melalui sebuah form yang ditampilkan melalui web dan memasukkan tipe data yang diinginkan dan data yang ingin dimasukkan. Batasan yang dilakukan dalam pembuatan perangkat lunak ini ialah:

a) Pengguna memasukkan data bertipe tertentu, kemudian data tersebut dienkripsi dengan algoritma yang sudah didefinisikan dan kuncinya beserta mode enkripsi. Setelah itu, data dimasukkan ke dalam basis data.
b) Pengguna menampilkan isi dari tabel tertentu setelah didekripsi dari basis data dengan kunci yang telah dimasukkan.

Perangkat lunak ini disusun atas lima modul utama, yaitu:

a) Modul Antarmuka
   Modul ini sendiri berbasis web yang dibuat dengan menggunakan ASP.NET dengan bahasa pemrograman C#.
b) Modul Pemrosesan *Query*
   Modul ini ialah penerapan dari pemrosesan *query* untuk memasukkan data ke dalam basis data dan mengambil data dari basis data. Karena operasi yang digunakan untuk melakukan pengujian hanya 2 yaitu memasukkan data dan menampilkan data, maka *query SQL* yang digunakan pun hanya dua, yaitu query "*INSERT INTO*" dan "*SELECT FROM*".
c) Modul Enkripsi – Dekripsi
   Modul ini ialah penerapan proses enkripsi dan dekripsi dengan algoritma yang telah didefinisikan pada subjudul 2.2.
d) Modul Fungsi Umum
   Modul ini digunakan untuk mendukung enkripsi dan dekripsi yang utama seperti pergeseran bit, pembalikan bit, dan operasi XOR. Selain itu, ada pula fungsi untuk melakukan pengubahan struktur data yang digunakan selama proses enkripsi dan dekripsi.

Selain itu, untuk mendukung proses dekripsi, dibutuhkan tabel tambahan dengan field:

Tabel 1. Field pada tabel tambahan untuk proses dekripsi

Kolom	Keterangan
Mode enkripsi	Digunakan untuk mencatat mode enkripsi yang digunakan (*ECB*, *CBC*, atau *CFB*)
Panjang kunci	Digunakan untuk validasi panjang kunci
IV	Digunakan untuk initial vector pada proses dekripsi
Panjang *padding*	Digunakan untuk menghilangkan *padding* pada proses dekripsi

Dalam proses enkripsi dan dekripsi, struktur data yang digunakan ialah dalam bentuk bit dan byte agar disimpan dapat ditampilkan kembali dalam web. Jadi, dalam sebuah tabel utama pengujian, memiliki korespondensi dengan tabel tambahan pada tabel 1 yang bersesuaian. Sebagai contoh, untuk record pertama pada tabel utama dengan key x akan bersesuaian dengan record pada tabel tambahan dengan key x pula. Dengan demikian, pada saat proses dekripsi sebuah record pada tabel utama, harus dicari terlebih dahulu record yang bersesuaian pada tabel tambahan agar dideteksi mode enkripsinya, divalidasi, kemudian dibaca *IV*-nya, dan dihilangkan *padding*-nya.

Keseluruhan proses algoritma perangkat lunak untuk melakukan pengujian ialah sebagai berikut:

a) Memasukkan data ke dalam basis data.
   1) Memilih mode block cipher yang digunakan (*ECB*, *CBC*, atau *CFB*).
   2) Memasukkan kunci.
   3) Menerima data dari pengguna yang akan dimasukkan ke dalam basis data.
   4) Mendefinisikan tipe data yang akan dimasukkan.
   5) Kemudian pengguna menekan tombol untuk memasukkan data yang telah diisikan ke basis data.
   6) Sebelum memasukkan data yang telah dimasukkan oleh pengguna ke dalam basis data, perangkat lunak melakukan enkripsi terlebih dahulu data dari pengguna.
   7) Data dimasukkan ke dalam basis data dalam keadaan terenkripsi.

b) Menampilkan data dari dalam basis data.
   1) Memilih tabel mana yang akan dilihat isinya.
   2) Kemudian pengguna menekan tombol untuk mengambil isi data dari dalam basis data.
   3) Sebelum menampilkannya, data yang diambil dari basis data didekripsi terlebih dahulu.
   4) Menampilkan data dari tabel yang telah dipilih oleh pengguna.

4. KESIMPULAN

Pengamanan data dengan menggunakan block cipher dapat dijadikan salah satu alternatif untuk mengenkripsi isi basis data yang pada umumnya menggunakan *stream cipher*.

Batasan-batasan dari perangkat lunak yang dihasilkan dari studi dan penerapan pengamanan dengan menggunakan *block cipher* pada basis data ialah tipe data yang berhasil dienkripsi dan didekripsi dengan baik ialah kelompok data teks (*character strings*) karena dalam representasi struktur datanya sama seperti mengenkripsi file biasa.

5. DAFTAR REFERENSI

[1] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition*, John Wiley & Sons, Inc, 1996.

[2] R. Munir, Diktat Kuliah IF5054 Kriptografi, Program Studi Teknik Informatika, STEI, ITB, 2006.

[3] G. Andrew Duthie, Microsoft ASP.NET Step by Step, Microsoft Press, 2002.

[4] Dicky Ekklesia, *Studi dan Implementasi Pengamanan Basis Data dengan Teknik Kriptografi Stream Cipher*, Laboratorium Ilmu dan Rekayasa Komputasi, Program Studi Teknik Informatika, STEI, ITB, 2005.