TEKNIK ENKRIPSI DAN DESKRIPSI MENGGUNAKAN ALGORITHMA *ELECTRONIC CODE BOOK (ECB)*

Ahmad Mufid
Program Studi Sistem Komputer Fakultas Teknik Universitas Sultan Fatah (UNISFAT)
Jl. Sultan Fatah No. 83 Demak Telpon (0291) 681024

Abstrak:. Keamanan teknologi dan sistem informasi menjadi sangat penting terutama terhadap data yang bersifat penting dan rahasia. Ada beberapa teknik penyandian (*enkripsi*) dan deskripsi kunci pengamanan baik secara konvensional maupun modern/kunci publik, diantanya adalah *electronic code book (ECD).* Teknik ini sangat sederhana tetapi cukup banyak digunakan karena mempunyai tingkat keamanan yang relatif baik.

Kata kunci : *password*, enkripsi, deskripsi, kriptografi, *electronic code book (ECD)*

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dalam sistem informasi. tetapi sering kurang mendapatkan perhatian dari pemilik dan pengelola sistem informasi, bahkan masalah sistem informasi dianggap nomor dua atau bahkan terakhir dari sederetan hal-hal penting yang berhubungan dengan sistem informasi.

Beberapa cara telah dikembangkan untuk menangani masalah keamanan ini, salah satu cara yang digunakan untuk menangani masalah ini adalah menggunakan algorithma penyandian data. Algorithma penyandian data saat ini jumlahnya semakin banyak seiring dengan perkembangan ilmu yang berhubungan dengan penyandian yang dikenal dengan istilah kriptografi. Dalam teknik ini data (*plaintext*) dirubah menjadi sandi (*ciphertext*) dengan menggunakan kunci tertentu. Untuk itu kerahasiaan kunci ini menjadi hal penting dalam keberhasilan penyandian ini.

Ada beberapa cara yang dapat digunakan dalam sistem kriptografi ini yaitu sistem konvensional/klasik dan sistem modern/kunci publik. Pada sistem kriptografi konvensional perubahan *plaintext* menjadi *ciphertex* menggunakan kunci yang sama, sedangkan sistem kriptografi kunci publik menggunakan dua kunci yang berbeda.

Dari berbagai algorithma kriptografi yang ada, maka akan digunakan algorithma *electronic code book (ECB)* untuk menyelesaikan tugas kuliah keamanan sistem informasi.

TINJAUAN PUSTAKA

Electronic Code Book (ECB)

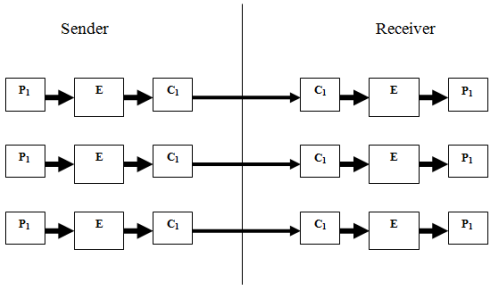
Pada sistem, setiap blok plainteks pi, dienkripsi secara individual dan independen menjadi blok cipherteks ci. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai Ci = Ek (Pi) sedangkan dekripsi sebagai Pi = Dk (Ci) Dalam hal ini, K adalah kunci dan Pi dan Ci masing-masing blok plainteks dan cipherteks ke-i.

Pada mode operasi ECB sebuah blok input plaintext dipetakan secara statis ke sebuah blok output ciphertext. Sehingga tiap plaintext yang sama akan menghasilkan ciphertext yang selalu sama pula. Sifat- sifat dari mode operasi ECB :

- Sederhana dan efisien
- Memungkinkan implementasi parallel
- Tidak menyembunyikan pola plaintext

Skema *Electronik Code Book (ECB)*

Adapun skema dari sistem kriptografi *electronic code book (ECB)* adalah sebagai berikut :



Gambar 1 : Skema algorithma ECB

Istilah “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 dari cipherteks yang berkoresponden. 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.

PEMBAHASAN

Algorithma Enkripsi *Electronic Code Book (ECB)*

Untuk membuat enkripsi (perubahan plainteks kedalam cipherteks dan) dengan menggunakan algorithma *Electronic Code Book (ECB)* dapat

dilakukan dengan langkah-langkah sebagai berikut :

1. Memasukkan plainteks
   Plainteks yang dimasukkan dapat berupa data teks, bilangan biner atau heksadesimal.
2. Bagi plainteks menjadi blok-blok yang berukuran 4 bit (plainteks sudah dibinerkan) atau dalam bentuk hexadesimal.
3. Tentukan kunci (K) yang akan digunakan (4 bit) atau dalam heksadesimal.
4. Gunakan fungsi enkripsi (E) dengan meng XOR-kan plainteks Pi dengan K.
5. Kemudian geser secara wrapping blok-blok cipherteks ke kiri satu persatu sehingga menghasilkan cipherteks secara lengkap.

Algorithma Deskripsi *Electronic Code Book (ECB)*

Untuk melakukan deskripsi cipherteks menjadi plainteks dilakukan dengan langkah-langkah sebagai berikut:

1. Menggeser secara wrapping blok-blok cipherteks ke kanan satu persatu.
2. Gunakan fungsi enkripsi E dengan meng-XOR-kan blok-blok cipherteks Ci dengan K.

Perhitungan Enkripsi Algorithma *Electronic Code Book (ECB)*

Misalkan dimasukkan sebuah plainteks : **MSI10**

Teks/ASCII : **MSI10** dapat dirubah menjadi bentuk desimal / biner / heksadesimal dengan hasil seperti terlihat dibawah ini.

M	S	I	1	0	ASCII
77	83	73	49	48	ECIMAL
4D	53	49	31	30	HEXA
01001101	01010011	01001001	00110001	00110000	BINER

Selanjutnya data biner tersebut dijadikan plainteks seperti terlihat dibawah ini.

01001101010100110100100100110001001100000 PLAIN

Bentuklah blok-blok plainteks (biner) tersebut kedalam 4 bit sehingga menjadi seperti dibawah ini.

0100 1101 0101 0011 0100 1001 0011 0001 0011 0000 BLOK

Selanjutnya, tentukan kunci K sebanyak 4 bit, misalkan ditentuka kuncinya adalah 1011.

1011 KEY

Gunakan fungsi enkripsi E dengan meng-XOR-kan blok-blok biner

plainteks Pi tersebut dengan kunci K. Adapun hasilnya dapat dilihat dibawah ini.

0100 1101 0101 0011 0100 1001 0011 0001 0011 0000	BLOK
1011 1011 1011 1011 1011 1011 1011 1011 1011 1011	KEY
1111 0110 1110 1000 1111 0010 1000 1010 1000 1011	XOR

Geser hasil operasi fungsi enkripsi XOR tersebut secara wrapping ke kiri satu persatu sehingga menghasilkan seperti ini.

1111 1100 1101 0001 1111 0100 0001 0101 0001 0111	GESER

Maka akan menghasilkan cipherteks seperti dibawah ini. Dalam contoh ini cipherteks di konversi dalam bentuk desimal dan heksadesimal.

252	209	244	21	23	DEC
FC	D1	F4	15	17	HEXA
1111 1100 1101 0001 1111 0100 0001 0101 0001 0111					CHIPER

Perhitungan Deskripsi Algorithma *Electronic Code Book (ECB)*

Geser cipherteks blok-blok biner secara wrapping ke kanan satu persatu sehingga terjadi seperti dibawah ini.

Cipherteks sebelum digeser.

1111 1100 1101 0001 1111 0100 0001 0101 0001 0111	CHIPER

Cipherteks setelah digeser.

1111 0110 1110 1000 1111 0010 1000 1010 1000 1011	GESER

Cipherteks blok-blok biner hasil pergeseran tersebut dilakukan operasi fungsi enkripsi E dengan cara meng-XOR-kan Ci tersebut dengan kunci K. Perhatikan hasil operasi tersebut dibawah ini.

1111 0110 1110 1000 1111 0010 1000 1010 1000 1011	GESER
1011 1011 1011 1011 1011 1011 1011 1011 1011 1011	KEY
0100 1101 0101 0011 0100 1001 0011 0001 0011 0000	XOR

Maka hasilnya sudah sama dengan plainteks awal.

0100 1101 0101 0011 0100 1001 0011 0001 0011 0000					PLAIN
01001101	01010011	01001001	00110001	00110000	BINER
M	S	I	1	0	ASCII
77	83	73	49	48	ECIMAL
4D	53	49	31	30	HEXA

KESIMPULAN

Dari hasil perhitungan enkripsi dan deskripsi algorithma *electronic code book (ECB)* tersebut diatas, maka dapat diperoleh kesimpulan bahwa metode cocok digunakan untuk pengamanan data yang diakses secara random. Jika terjadi kesalahan pada blok-blok cipherteks tertentu maka tidak akan mempengaruhi proses pada blok-blok cipherteks yang lainnaya.

Kelemahan metode ini adalah plainteks sering berulang-ulang sehingga menghasilkan enkripsi cipherteks yang sama.

Untuk mengatasi hal tersebut dapat dibuat kunci K yang lebih besar, misalnya 64 bit sehinga potensi terulangnya plainteks dan hasil enkripsi cipherteks semakin kecil. Selain itu juga dapat dilakukan pengaturan ulang

enkripsi tiap blok individual bergantung pada semua blok sebelumnya, sehingga plainteks yang identik akan menghasilkan cipherteks yang berbeda.

DAFTAR PUSTAKA

Munir R., 2006, *Kriptografi*, Yogyakarta, Andi Ofset

Rachmatsyah A., 2005, *Sistem Kriptografi Kunci Publik Berbasis Diophantine*, Bandung, Tugas Kuliah Keamanan Sistem Lanjut Magister Teknik Komputer Institut Teknologi Bandung (tidak dipublikasikan)

Sediyono E., 2010, *Keamanan Sistem Informasi, Semarang*, Materi Kuliah Magister Sistem Informasi Universitas Diponegoro (tidak dipublikasikan)

Setyaningsih E.,__, *Kriptografi*, Bandung, Materi Kuliah Magister Teknik Komputer Institut Teknologi Bandung (tidak dipublikasikan)

Tjiharjadi S. Dan Wijaya M. C., 2009, *Pengamanan Data Menggunakan Metode Enkripsi Simetri dengan Algorithma FEAL*, Yogyakarta, Seminar Nasional Aplikasi Teknologi Informasi.