Jurnal Matematika Vol.6 No.1
Nopember 2006 [77 - 84]

ALGORITMA DATA ENCRYPTION STANDARD (DES) PADA ELECTRONIC CODE BOOK (ECB)

Yurika Permanasari, Erwin Harahap

Jurusan Matematika, UNISBA, Jalan Tamansari No 1, Bandung,40116, Indonesia
yurika71@yahoo.com

Jurusan Matematika, UNISBA, Jalan Tamansari No 1, Bandung,40116, Indonesia
erwin2h@yahoo.com

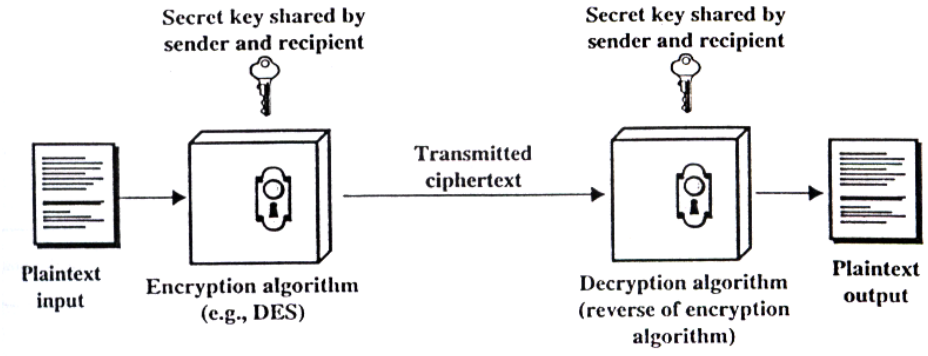
Abstrak. *Electronic Code Book* (ECB) adalah salah satu mode enkripsi yang menggunakan algoritma *Data Encryption Standard* (DES) dalam enkripsi datanya. Dalam mode *Electronic Code Book* (ECB), 64 bit (1 blok) plainteks di-enkripsi secara bersamaan dan setiap blok plainteks di-enkripsi menggunakan kunci yang sama. *Electronic Code Book* (ECB) cukup efektif digunakan pada pesan–pesan singkat. Jika plainteks lebih besar dari 64 bit maka input data dibagi per-64 bit, jika diperlukan dapat ditambah *padding* atau bit pelengkap tanpa merubah makna pesan pada alur blok untuk menggenapkan menjadi 64 bit.

Kata kunci : enkripsi; dekripsi; plainteks; Ciperteks

1. Latar Belakang

Bertambahnya penggunaan komputer dan sistem komunikasi oleh industri telah menambah resiko sebuah informasi yang bersifat pribadi. Resiko ini merupakan ancaman yang memerlukan keamanan, Enkripsi adalah suatu metode utama perlindungan informasi elektronik yang berharga. Sejauh ini, terdapat dua bentuk enkripsi yang biasa digunakan yaitu enkripsi konvensional (enkripsi simetrik) dan enkripsi *public-key* (enkripsi asimetrik). Salah satu algoritma enkripsi simetrik yang paling umum digunakan adalah *Data Encryption Standard* (DES).

Enkripsi simetrik mempunyai lima komposisi, yang ditunjukkan dalam gambar berikut :



Gambar 1. Model Sederhana Enkripsi Konvensional

2. Electronic Code Book (ECB)

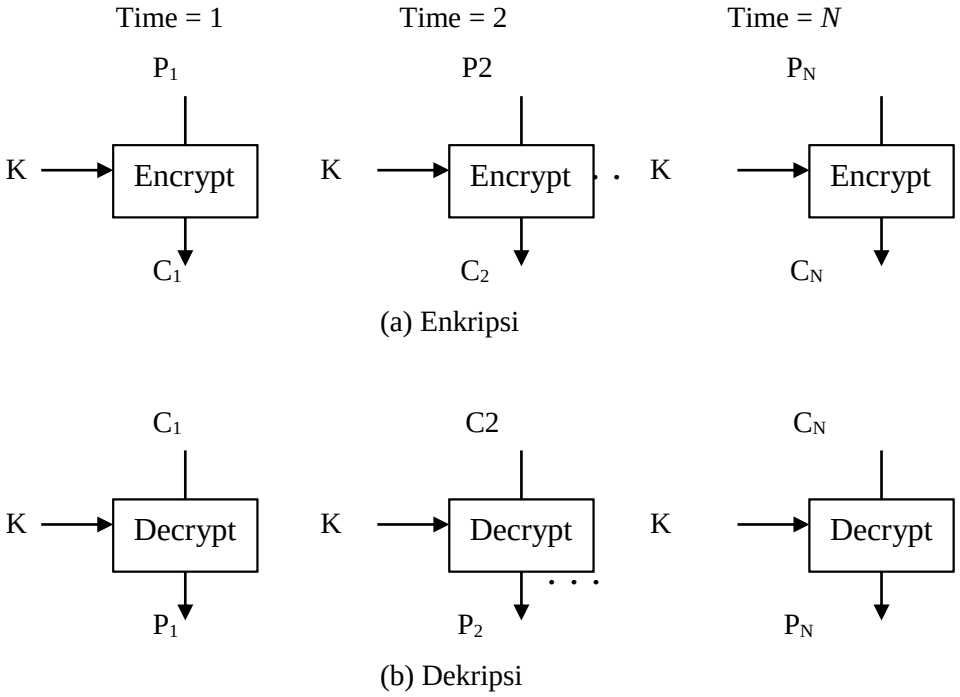
Electronic code Book (ECB) adalah salah satu mode enkripsi yang menggunakan algoritma *Data Encryption Standard* (DES) dalam enkripsi datanya. Dalam mode *Electronic code Book* (ECB), 64-bit (1 blok) plainteks di-enkripsi secara bersamaan dan setiap blok plainteks di-enkripsi menggunakan kunci yang sama. Istilah *code Book* (ECB) itu dipakai, karena untuk kunci yang diberikan terdapat cipherteks yang unik untuk setiap blok plainteks 64-bit nya,

sehingga untuk sebuah *codeBook* yang sangat besar pasti terdapat pola plainteks 64-bit yang cocok dengan cipherteksnya.

Untuk pesan yang lebih dari 64-bit prosedurnya sangat mudah yaitu dengan membagi pesan–pesan tersebut kedalam blok 64-bit. Jika dibutuhkan dapat ditambahkan *padding* atau bit pelengkap pada akhir blok untuk menggenapkan 64-bit.

Electronic code Book (ECB) adalah Mode *Data Encryption Standard* (DES) yang paling sederhana, dimana Enkripsi dilakukan hanya dengan menjalankan tahap-tahap berikut :

1. Rubah plainteks dengan menerapkan Permutasi awal / *Initial Permutation* (IP) sehingga didapat L_0 dan R_0 (dalam biner)
2. Gunakan kunci sesuai aturan key generation
3. Enkripsi dilakukan 16 *round* dimana setiap *round* sesuai aturan *round* pada *Data Encryption Standar* (DES)
4. Gunakan aturan Invers Permutasi Awal / Inverse Initial Permutation (IP^{-1}) sehingga didapat R_{16} dan L_{16}
5. Cipherteks sama dengan gabungan dari R_{16} dan L_{16}

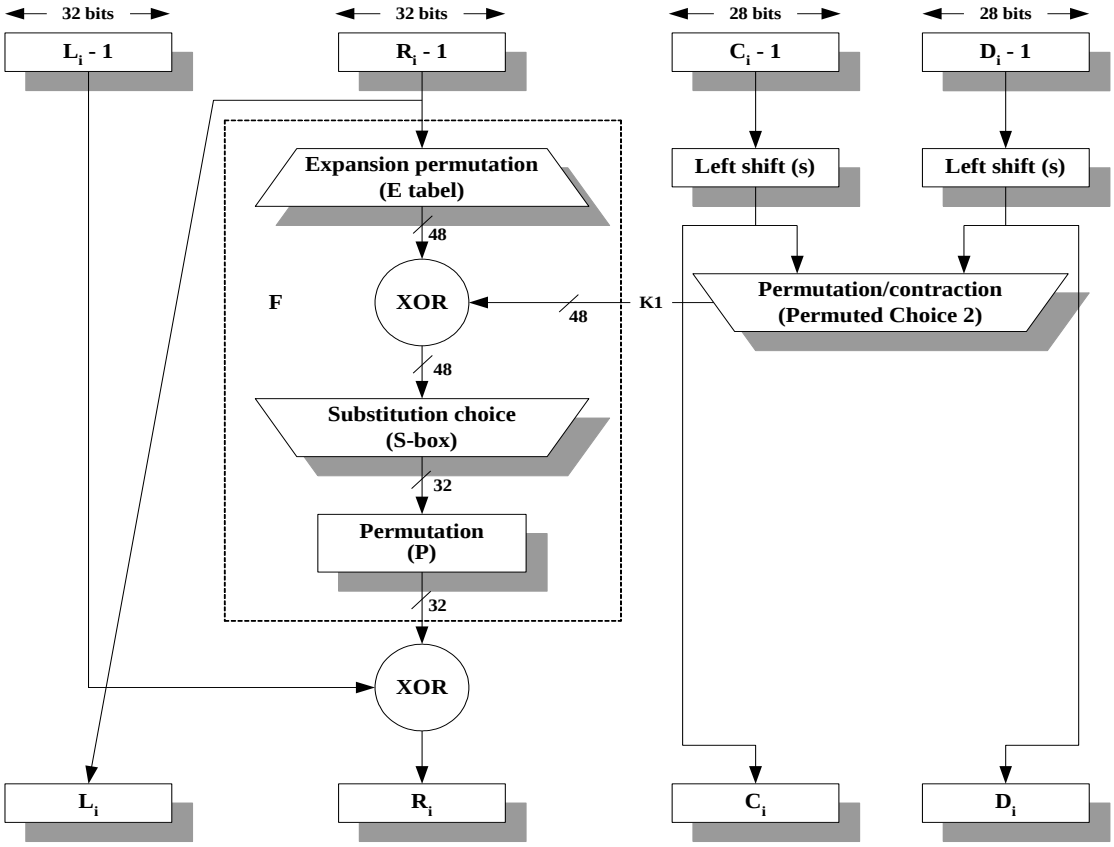


Gambar 2. Mode Electronic Code Book (ECB)

Untuk pesan yang lebih panjang dari 64 bit, prosedurnya merubah pesan menjadi blok-blok yang memuat 64 bit. Dekripsi pada ECB dilakukan per blok pada waktu yang sama menggunakan kunci yang sama dengan enkripsi yang berbeda setiap *round*.

3. Enkripsi DES

Aturan umum dari fungsi *Data Encryption Standard* (DES) dalam algoritma enkripsi menggunakan diagram alur (flow chart) dibawah ini :



Gambar 3 **Round tunggal dari algoritma *Data Encryption Standard* (DES)**

Jika melihat gambar diatas, bagan terbagi dua menjadi fungsi enkripsi plainteks dan penurunan kunci. Plainteks sebagai input awal untuk enkripsi DES adalah 64 bit. Bitstring ini dibagi 2 bagian menjadi R_0 dan L_0 yang masing – masing 32 bit. Sedangkan untuk penurunan kunci juga menggunakan 64 bit yang kemudian mengalami permutasi menjadi 56 bit. Berikut adalah tabel-tabel yang digunakan dalam penurunan kunci ;

Table 1 **DES Key schedule Calculation**

(a) Input key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

(b) Permuted Choice One (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	28
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

(c) Permuted Choice Two (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Setelah dilakukan left shift maka bitnya melalui tahap Permuted Choice Two (PC-2) melalui aturan tabel berikut, adapun aturan berapa bit yang harus berpindah secara circular sesuai dengan tabel dibawah ini :

Table 2 **Schedule Of Left Shifts**

Round number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Fungsi F pada enkripsi mengambil input pertamanya sebagai argumen R_0 yang merupakan *bitstring* dengan panjang 32 dan argumen keduanya yaitu L_0 juga *bitstring* dengan panjang 32, kemudian menjalankan langkah-langkah berikut:

1. Argumen pertama diekspansi menjadi bitstring dengan panjang 48 menggunakan tabel *expansion permutation* (E). R_0 dimana permutasi dilakukan sedimikian rupa sehingga 16 bitnya muncul 2 kali.

2. Hitung $E(R_0) \oplus$ dengan K dan hasilnya ditulis sebagai gabungan dari delapan 6 bit string B = $B_1B_2B_3B_4B_5B_6B_7B_8$.

3. Langkah berikutnya menggunakan delapan S-box yaitu S_1, ..., S_8. Setiap S_1 ditetapkan memiliki 4 X 16 barisan yang yang berisi nilai bilangan bulat antara 0 -15. Setelah didapat bitstring dengan panjang 6, misalnya $B_j = b_1b_2b_3b_4b_5b_6$, hitung $S_j(B_j)$ sebagai berikut:
   Setiap dua bit b_1b_6 ditentukan sebagai representasi biner baris r pada S_j $(0 \le r \le 3)$, dan empat bit $b_2b_3b_4b_5$ ditentukan sebagai representasi kolom c pada S_j $(0 \le c \le 15)$, sehingga $S_j(B_j)$ didefinisikan sebagai masukan S_j (r, c) ditulis dalam biner sebagai bitstring dengan panjang empat . dengan cara ini dihitung: $C_j = S_j(B_j)$, $1 \le j \le 8$.

4. *Bitstring* C = $C_1C_2C_3C_4C_5C_6C_7C_8$ dengan panjang 32 yang dipermutasikan menggunakan tabel permutasi C yang telah ditentukan. Hasil bitstring P(C) didefinisikan sebagai $f(R_0, K)$.

Berikut adalah tabel-tabel yang digunakan dalam enkripsi :

Tabel 3 **Initial Permutation (IP)**

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	7
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	23	5
63	55	47	39	31	23	15	7

Tabel 4 **Expansion Permutation (E)**

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

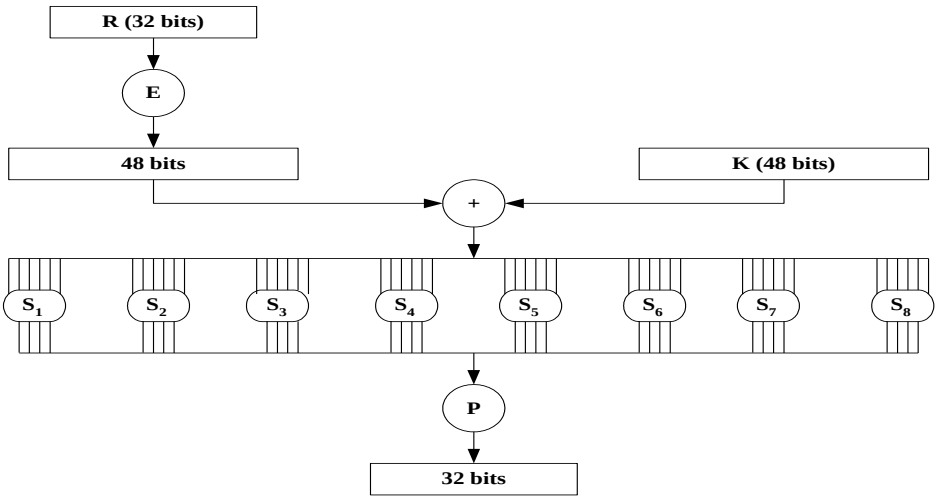
Tabel 5 **Permutation Function (P)**

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	17	3	9
19	13	30	6	22	11	4	25

Tabel 6 **Inverse Initial Permutation (IP^{-1})**

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Peran S-box pada fungsi F digambarkan dalam gambar 4. Subtitusi terdiri dari sebuah himpunan 8 buah S-box, untuk setiap S-boxnya disepakati 6 bit sebagai input dan menghasilkan 4 bit sebagai output.



Gambar 4 **Calculation of F(R, K)**

Perubahan bentuk ini digambarkan dalam tabel 7 yang ditafsirkan sebagai berikut: bit pertama dan terakhir dari input dalam box S_i membentuk 2-bit angka biner untuk memilih 1 dari 4 substitusi yang digambarkan oleh 4 baris dalam tabel S_i, 4 bit ditengah memilih 1 dari 16

kolom. Nilai desimal dalam sel yang dipilih oleh baris dan kolom kemudian diganti kedalam gambaran 4 bit untuk menghasilkan output. Contoh dalam S_1, untuk input 011001, barisnya adalah 01 (baris 1) dan kolomnya adalah 1100 (kolom 12). Nilai dalam baris 1, kolom 12 adalah 9, jadi outputnya adalah 1001.

***Tabel 7* definition of DES S-boxes**

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	2	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Untuk mengetahui kembali data yang telah di-enkripsi maka digunakan algoritma dekripsi. Dekripsi juga menggunakan algoritma yang sama seperti enkripsi, kecuali penerapan / aplikasi subkuncinya dibalikkan.

4. Contoh Kasus :

Diketahui beberapa input dibawah ini :

- Data Plainteks 64-bit yaitu ADE DEFA BACA BAB 12 (dalam biner):

  1010110111101101111011111010101110101100101010111010101 1 00010010

- Input Kunci 64-bit yaitu 145BC778FF16D39E (dalam biner):

  0001010001011011110001110111100011111111000101101101001 1 10011110

Maka proses pencarian chiperteks yang terjadi ditunjukkan dalam satu *round*, sebagai berikut:

Dimulai dengan penggunaan tabel IP , maka akan menghasilkan (dalam biner):

L_0 = 00000110100000000001011101101111
$L_1 = R_0$ = 01111111011111110111111111101100

Round 1:

$E(R_0)$ = 001111111110101111111110101111111111111101011000
K_1 = 101111110000011010001110111011100011101110001110
$E(R_0) \oplus K_1$ = 100000001110110101110000010100011100010011010110
S-box outputs 010001001110111100110101001111 10
$f(R_0, K_1)$ = 101010100100001110110101111111 00
$L_2 = R_1$ = 10101100110000111010001010010011
IP^{-1} = 011100110111101111010101110101010101001111011101 0
11101001010111

Setelah melalui 16 *round* enkripsi, maka diperoleh data cipherteks dari plainteks ADEDEFABACABAB12 yaitu B9BDEAEAA9EEBA57.

5. Kesimpulan

Electronic CodeBook (ECB) adalah mode yang paling sederhana untuk meng-enkripsi data dengan menggunakan algoritma *Data Encryption Standard* (DES). Plainteks pada *Electronic CodeBook* (ECB) di-enkripsi per blok dimana setiap blok berisi 64 *bitstring* dengan menggunakan kunci yang sama. Besar kunci yang digunakan adalah 64-bit, enkripsi dilakukan secara iterasi sebanyak 16 *round.*

Jika plainteks *Electronic CodeBook* (ECB) lebih besar dari 64 bit maka input data dibagi per-64 bit, jika diperlukan dapat ditambahkan *padding* atau bit pelengkap tanpa merubah makna pesan pada alur blok untuk menggenapkan menjadi 64 bit.

Electronic CodeBook (ECB) cukup efektif digunakan pada pesan– pesan singkat. Untuk pesan yang panjang, keamanan mode *Electronic CodeBook* (ECB) mungkin tidak akan terjamin, karena jika muncul lebih dari satu pesan 64 bit yang sama, maka akan menghasilkan cipherteks yang sama. Sehingga jika suatu pesan mempunyai unsur-unsur yang berulang (dengan pengulangan periode sebuah perkalian 64 bit), maka unsur–unsur tersebut mudah di identifikasi

oleh kriptoanalis. Ini mungkin membantu dalam menganalisis atau mungkin kesempatan untuk mensubstitusi atau mengatur blok. Oleh karena itu untuk data plainteks yang lebih besar dari 64 bit maka disarankan menggunakan mode dan algoritma lain yang lebih menjamin keamanan data.

Daftar Pustaka

Barker, (1991). W.Introduction to the Analysis of the Data Encryption Standard (DES), Laguna Hills, CA; Aegean Park Press, 1991.

Coppersmith, (1994). D. "The Data Encryption Standard (DES) and Its Strength Against Attacks, "IBM Journal of Research and Development, May 1994.

Stallings, (2003). William, Cryptography and Network Security, Third Edition, Pearson Education,Inc, 2003.

Stinson, (1956). D.R. Cryptography: theory and practice, University of Nebraska ,licoln, 1956.

Int., **7**: 489–495.