

Bahan kuliah IF4020 Kriptografi

Review Beberapa Block Cipher dan Stream Cipher (Bagian 3: Triple DES dan RC5)

Oleh: Dr. Rinaldi Munir

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
ITB



Triple DES

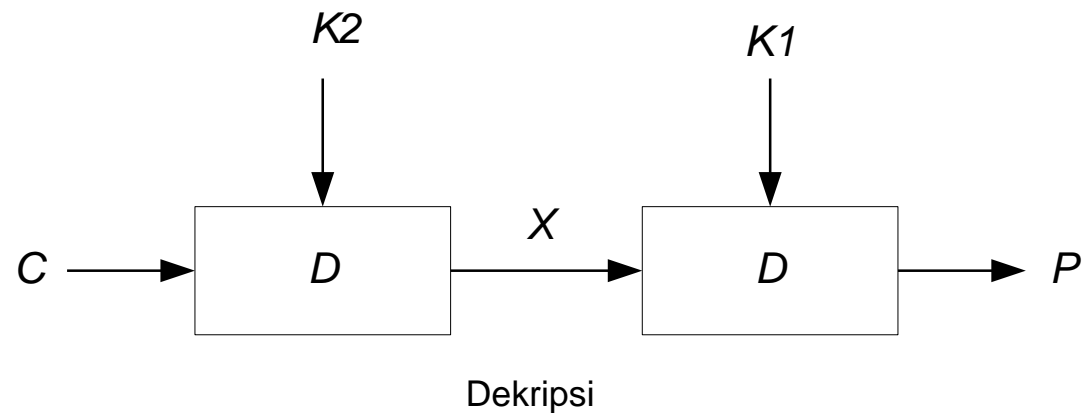
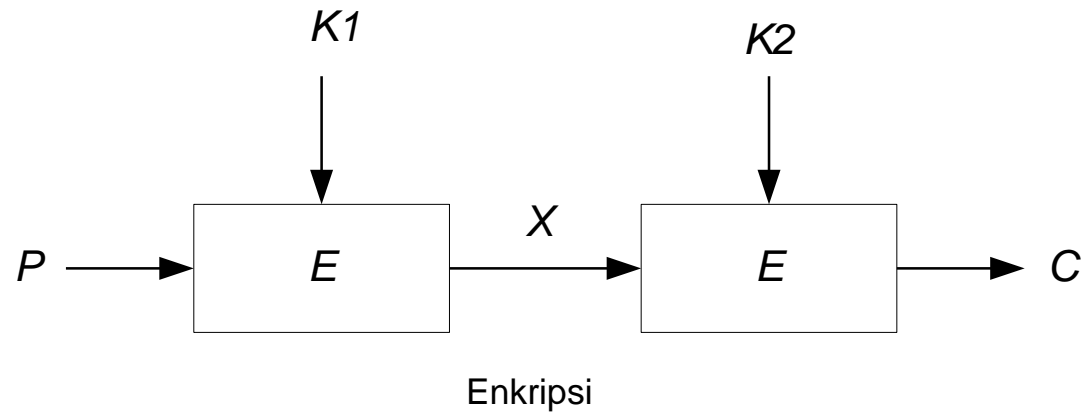
DES Berganda

- Karena DES mempunyai potensi kelemahan pada *brute force attack*, maka dibuat varian dari DES.
- Varian DES yang paling luas digunakan adalah DES berganda (*multiple DES*).
- DES berganda adalah enkripsi berkali-kali dengan DES dan menggunakan kunci ganda.

- Tinjau DES berganda:
 1. *Double DES*
 2. *Triple DES*

Double DES

- Menggunakan 2 buah kunci eksternal, K_1 dan K_2 .
- Enkripsi: $C = E_{K_2}(E_{K_1}(P))$
- Dekripsi: $P = D_{K_1}(D_{K_2}(C))$



- Kelemahan *Double DES*: serangan *meet-in-the-middle attack*:
- Dari pengamatan,

$$C = E_{K_2}(E_{K_1}(P))$$

maka

$$X = E_{K_1}(P) = D_{K_2}(C)$$

- Misalkan kriptanalis memiliki potongan C dan P yang berkoreponden.
- Enkripsi P untuk semua kemungkinan nilai K_1 (yaitu sebanyak 2^{56} kemungkinan kunci). Hasilnya adalah semua nilai X
- Simpan semua nilai X ini di dalam tabel

- Berikutnya, dekripsi C dengan semua semua kemungkinan nilai $K2$ (yaitu sebanyak 2^{56} kemungkinan kunci).
- Bandingkan semua hasil dekripsi ini dengan elemen di dalam tabel tadi. Jika ada yang sama, maka dua buah kunci, $K1$ dan $K2$, telah ditemukan.
- Tes kedua kunci ini dengan pasangan plainteks-cipherteks lain yang diketahui. Jika kedua kunci tersebut menghasilkan cipherteks atau plainteks yang benar, maka $K1$ dan $K2$ tersebut merupakan kunci yang benar

Triple DES (TDES)

- Menggunakan DES tiga kali
- Bertujuan untuk mencegah *meet-in-the-middle attack*.
- Bentuk umum TDES (mode EEE):

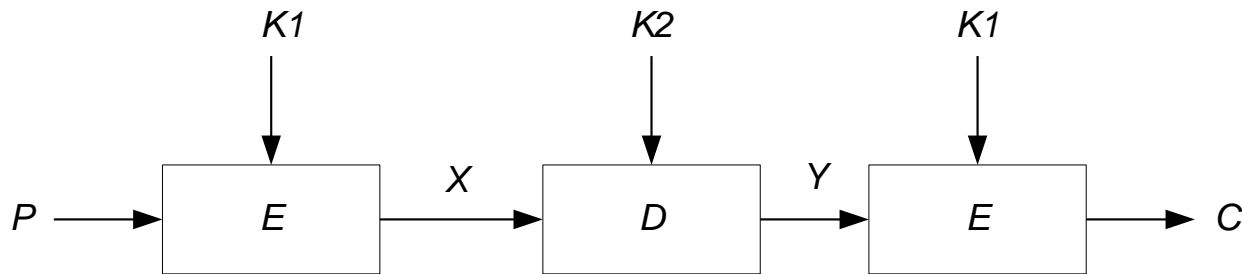
$$\text{Enkripsi: } C = E_{K_3}(E_{K_2}(E_{K_1}(P)))$$

$$\text{Dekripsi: } P = D_{K_1}(D_{K_2}(D_{K_3}(C)))$$

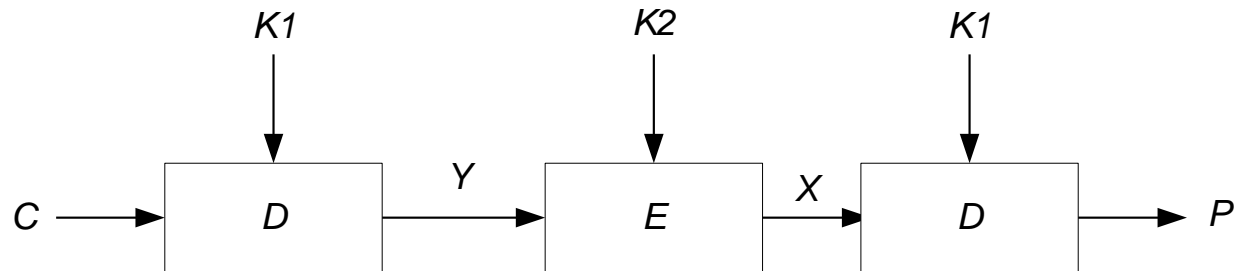
- Untuk menyederhanakan TDES, maka langkah di tengah diganti dengan D (mode EDE).
- Ada dua versi TDES dengan mode EDE:
 - Menggunakan 2 kunci
 - Menggunakan 3 kunci

Triple DES

Triple DES dengan 2 kunci

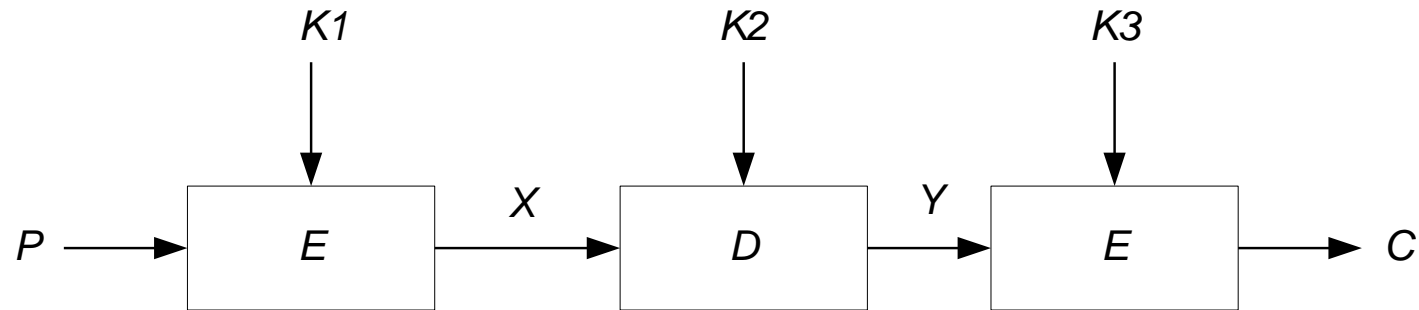


Enkripsi

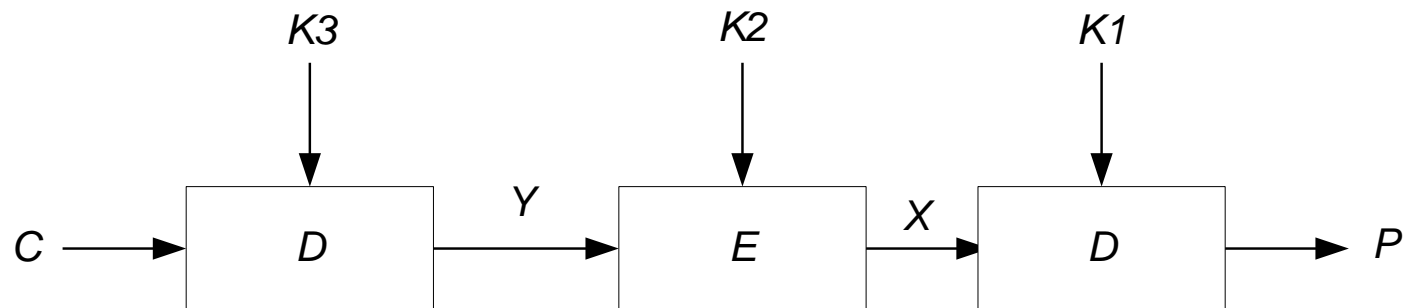


Dekripsi

Triple DES dengan 3 kunci



Enkripsi



Dekripsi

RC5

- *RC5* dibuat oleh Ron Rivest dari Laboratorium *RSA*.
- Tidak seperti algoritma *cipher* blok lainnya, *RC5* mempunyai:
 - ukuran blok yang variabel (32, 64, atau 128 bit)
 - panjang kunci yang variabel (0 sampai 2040 bit)
 - dan jumlah putaran yang variabel (0 sampai 255).

Parameter	Simbol	Nilai yang dibolehkan
Ukuran blok (dalam bit)	w	16, 32, 64
Jumlah putaran	r	0, 1, ..., 255
Panjang kunci eksternal K (dalam <i>byte</i> , 1 <i>byte</i> = 8 bit)	b	0, 1, ..., 255

Pembentukan Kunci Internal

- Kunci internal ada sebanyak $2r + 2$ buah yang masing-masing disimpan di dalam elemen-elemen larik yang dilabeli sebagai $S[0], S[1], \dots, S[t - 1]$ dengan $t = 2r + 2$.
- Setiap elemen larik panjangnya satu *word* (1 *word* = w bit)

- Mula-mula, semua *byte* dari kunci eksternal, $K[0..b - 1]$, disalin ke dalam larik L yang berukuran c *word*, $L[0..c - 1]$
- lalu *padding* dengan sejumlah 0 jika perlu (*padding* terjadi jika b bukan kelipatan w).
- Kemudian inisialisasi larik S sebagai berikut:

$S[0] \leftarrow P_w$

for $i \leftarrow 1$ **to** $t - 1$ **do**

$S[i] \leftarrow S[i - 1] + Q_w$

endfor

yang dalam hal ini nilai P_w dan Q_w (dalam heksadesimal) berbeda-beda bergantung pada w sebagai berikut [STA98]:

w	16	32	64
P_w	B7E1	B7E15163	B7E151628AED2A6B
Q_w	9E37	9E3779B9	9E3779B97F4A7C15

Konstanta P_w dan Q_w didasarkan pada representasi bilangan alam e dan ϕ dalam biner,

$$P_w = \text{Odd}[(e - 2)2^w]$$

$$Q_w = \text{Odd}[(\phi - 1)2^w]$$

yang dalam hal ini,

$$e = 2.718281828459\dots$$

$$\phi = 1.618033988749\dots = \frac{1 + \sqrt{5}}{2}$$

Akhirnya, campurkan L dan S sebagai berikut:

```
i ← 0
j ← 0
X ← 0
Y ← 0
n ← 3 * max(r, c)
for k ← 1 to n do
    S[i] ← (S[i] + X + Y) <<< 3
    X ← S[i]
    i ← (i + 1) mod (t)
    L[j] ← (L[j] + X + Y) <<< ( X + Y)
    Y ← L[j]
    j ← (j + 1) mod (c)
endfor
```

Enkripsi

- Tinjau *RC5* dengan ukuran blok 64 bit dan jumlah putaran r .
- Enkripsi menggunakan kunci internal $S_0, S_1, \dots, S_{2r+2}$ yang masing-masing panjangnya 32-bit.
- Dua kunci internal digunakan untuk setiap putaran $i = 1, 2, \dots, r$ dan dua buah kunci internal tambahan sebelum putaran pertama jadi seluruhnya ada $2r + 2$ buah kunci internal).
- Untuk melakukan enkripsi, mula-mula blok plainteks dibagi menjadi 2 bagian, A dan B , yang masing-masing panjangnya 32 bit. Kemudian masing-masing bagian dijumlahkan (dalam modulo 2^{32}) dengan S_0 dan S_1 :

$A \leftarrow A + S[0]$

$B \leftarrow B + S[1]$

- Selanjutnya untuk setiap putaran dari 1 sampai r dilakukan operasi *XOR*, pergeseran ke kiri secara sirkuler, dan penjumlahan dalam modulo 2^{32} dengan kunci internal sebagai berikut:

for $i \leftarrow 1$ **to** r **do**

$A \leftarrow ((A \oplus B) \lll B) + S[2i]$

$B \leftarrow ((B \oplus A) \lll A) + S[2i+1]$

endfor

Cipherteks pada putaran terakhir disimpan di dalam A dan B .

Gabungan keduanya adalah blok plainteks yang berukuran 64 bit.

Proses enkripsi satu putaran:

