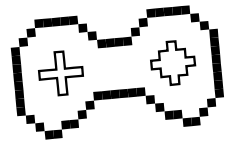
Praktikum Kriptografi

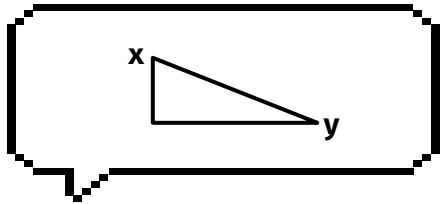
Pertemuan - 09

Topik: DES, S-DES

Review



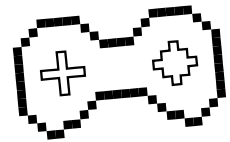
- **RSA**



DES

(Data Encryption Standard)

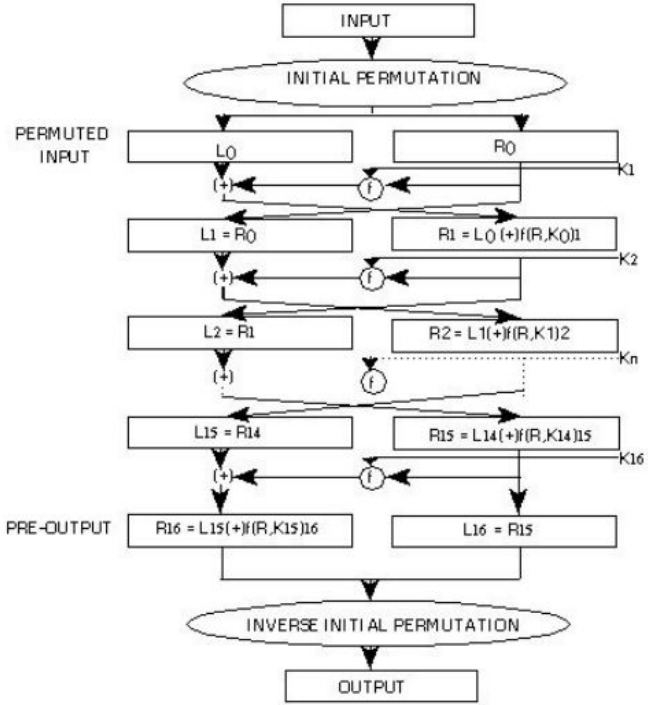
Algoritma DES



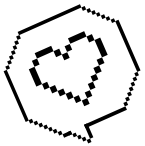
- DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok.
- DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit ciphertext dengan menggunakan 56 bit kunci internal (internal key) atau sub-kunci (subkey).
- Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

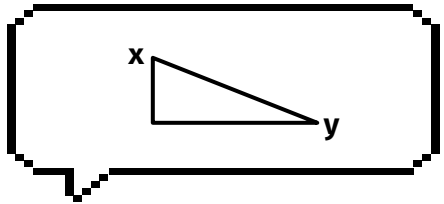
Algoritma DES

- Blok plaintext dipermutasi dengan matriks permutasi awal (IP).
- Hasil permutasi awal kemudian di-enchipering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
- Hasil enchipering kemudian dipermutasi dengan matriks permutasi balikan (IP-1)



S-Des Aja Lah Ya



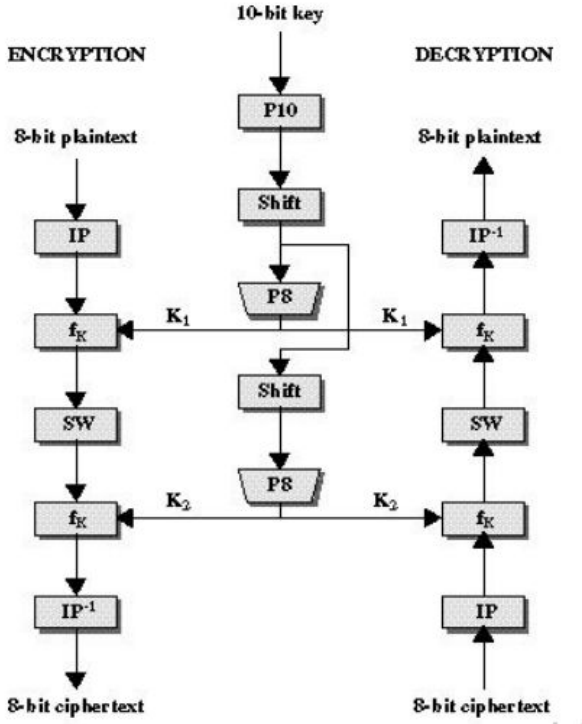


S-DES

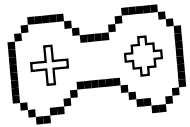
(Simplified Data Encryption Standard)

Algoritma S-DES

- S-DES (Simplified-Data Encryption Standard) lebih sederhana, melibatkan 8 bit plaintext-ciphertext, dan 10 bit kunci saja.



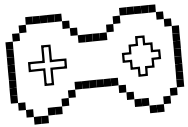
Contoh Key Generation



Diketahui:

- Plaintext : B (ASCII : 66 → 01000010) ⟶ 8 bit
- Master Key : y (ASCII : 121 → 01111001 + 01 → 0111100101) ⟶ 10 bit
- P_{10} : 3 5 2 7 4 10 1 9 8 6
- P_{8} : 6 3 7 4 8 5 10 9
- P_{4} : 2 4 3 1

Cari Kunci K1 dan K2

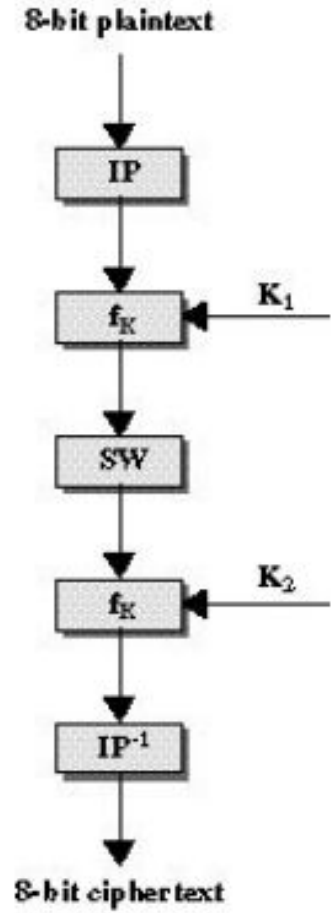


1. Key : 0 1 1 1 1 0 0 1 0 1
   Acak key sesuai P_{10}
   - P_{10} : 3 5 2 7 4 10 1 9 8 6
   - Key : 1 1 1 0 1 1 0 0 1 0
2. Bagi 2 P_{10}, geser kiri hasil P_{10} sebanyak 1x
   - Ls1 : 1 1 0 1 1 ||| 0 0 1 0 1
3. Ls_1 diacak dengan P_8, hasilnya adalah K1
   - P8 : 6 3 7 4 8 5 10 9
   - **K1 : 0 0 0 1 1 1 1 0**

Untuk cari K2:

1. Ls_1 digeser 2x jadi Ls_2
   - Ls_2 : 0 1 1 1 1 ||| 1 0 1 0 0
2. Acak hasil Ls_2 dengan P_8, jadilah K2
   - P8 : 6 3 7 4 8 5 10 9
   - **K2 : 1 1 0 1 1 1 0 0**

Enkripsi



Plaintext : 01000010

IP : 26314857

: 10000001

0101 0001

SW : 0001 0101

Ep : 41232341

: 10000010

K_1 : 00011110 XOR

10011100

S_0 : 1001 S_1 : 1100

Rn : 11 Rn : 10

Cn : 00 Cn : 10

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

	0	1	2	3
0	0	0	1	2
1	2	0	1	3
2	3	0	1	0
3	3	2	1	0

11 00

P4 : 2431

: 1101

1000 XOR

0101

Ep : 41232341

: 10101010

K_2 : 11011100 XOR

01110110

S_0 : 0111 S_1 : 0110

Rn : 01 Rn : 00

Cn : 11 Cn : 11

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

	0	1	2	3
0	0	0	1	2
1	2	0	1	3
2	3	0	1	0
3	3	2	1	0

00 11

P4 : 2431

: 0110

0001 XOR

0111 0101

IP^{-1} : 41357286

CT : 10100111

Enkripsi

1. Plainteks 8 bit diacak dengan IP

Plaintext : 01000010

IP : 26314857

: 10000001

2. Ambil 4 BIT PALING KANAN, lakukan expansion permutation (Ep) lalu XOR dengan K1

Ep : 41232341

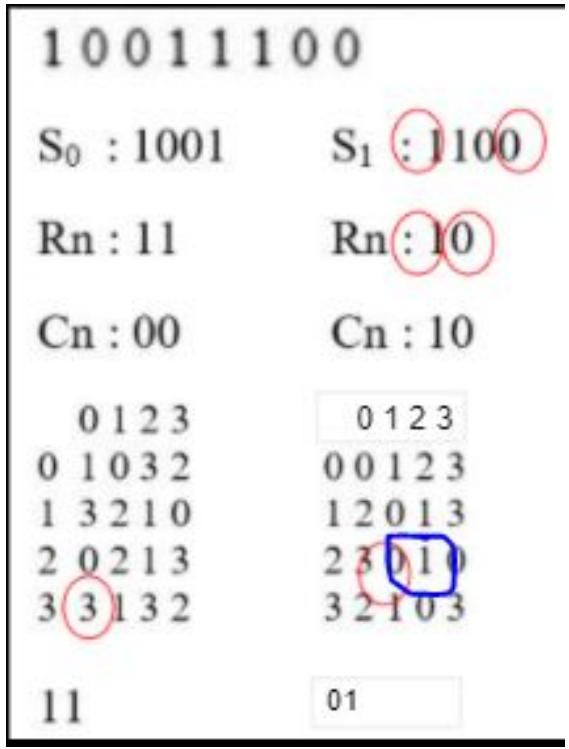
: 10000010

K_1 : 00011110 XOR

10011100

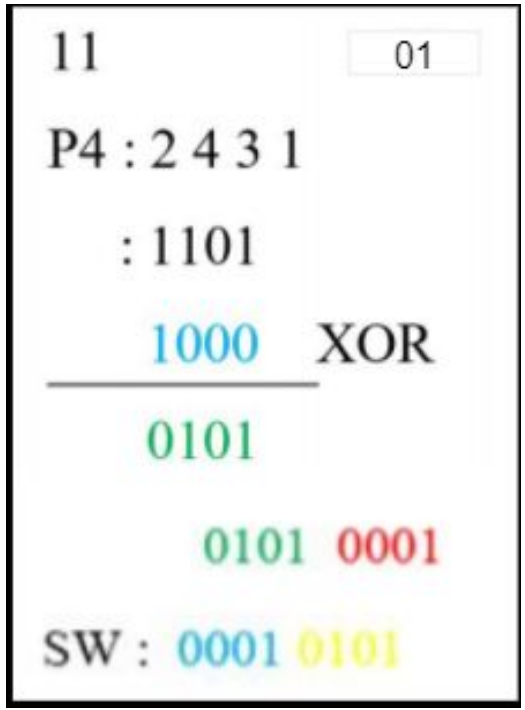
Enkripsi

- Hasil XOR dengan K1 tadi akan masuk ke substitution box
- Bagi 2 jadi S0 dan S1, cari Rn dan Cn
- Gunakan Rn (Row) dan Cn (Column) untuk memilih angka pada box
- Hasilnya jadi biner 2 digit



Enkripsi

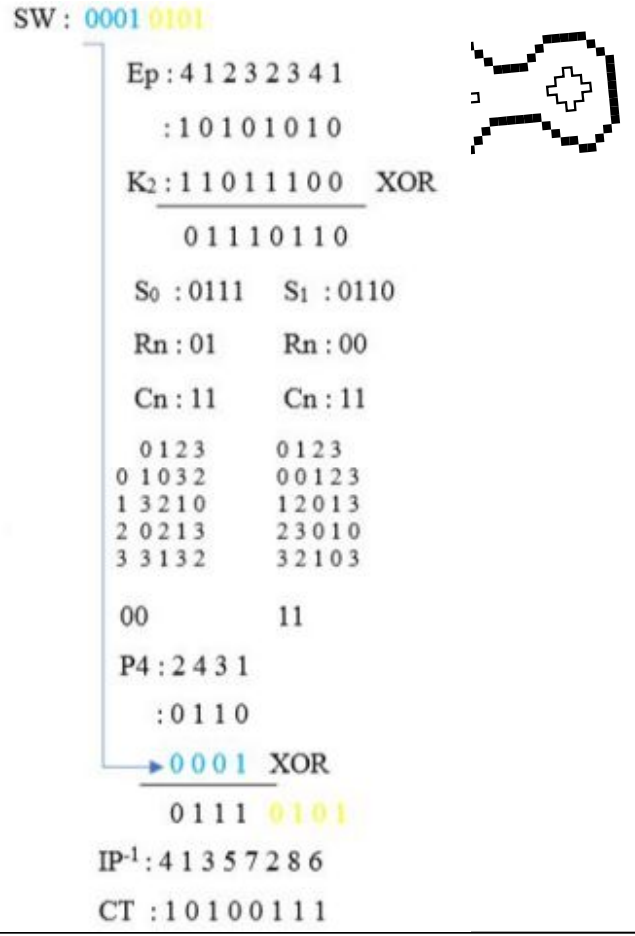
- Hasil Box diacak oleh P4 dan di XOR oleh 4 BIT KIRI DARI HASIL IP DI AWAL
- Gabungkan dengan 4 BIT KANAN HASIL IP lalu lakukan Swap (SW)



Enkripsi

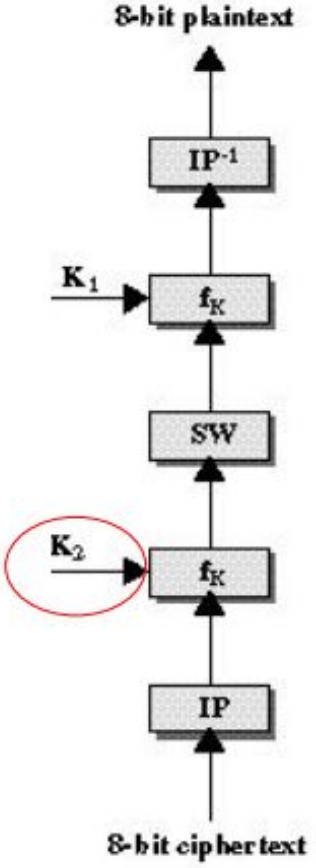
- Lanjutkan langkah serupa dengan K2

- Acak dengan IP- untuk mendapatkan ciphertext



Dekripsi

Sama kek enkripsi
tapi dari K2 dulu



Dekripsi

CipherText : 10100111

IP : 26314857

: 01110101

0001 0101

SW : 0101 0001

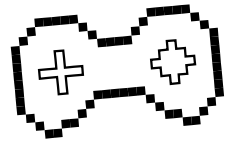
Ep : 41232341	Ep : 41232341
: 10101010	: 10000010
K2 : 11011100 XOR	K1 : 00011110 XOR
01110110	10011100
S0 : 0111 S1 : 0110	S0 : 1001 S1 : 1100
Rn : 01 Rn : 00	Rn : 11 Rn : 10
Cn : 11 Cn : 11	Cn : 00 Cn : 10
0123 0123 0 1032 00123 1 3210 12013 2 0213 23010 3 3132 32103	0123 0123 0 1032 00123 1 3210 12013 2 0213 23010 3 3132 32103
00 11	11 01
P4 : 2431	P4 : 2431
: 0110	: 1101
0111 XOR	0101 XOR
0001	1000 0001

K2

IP-1 : 41357286

PT : 01000010 (B)

Tugas



1. Enkripsikan huruf paling depan nama kalian (KAPITAL) dengan terlebih dahulu mengkonversikan ke ASCII (M: 77 = 01001101). Sebagai kunci gunakan huruf terakhir nama kalian (HURUF KECIL) yang telah dikonversi ke ASCII dan tambahkan 01 di belakangnya (l: 108 = 01101100+01 = 0110110001)

(Contoh: Pt = M, Ct = l)

2. Dekripsikan kembali hingga didapatkan kedua huruf tersebut (M dan l), dengan mengerjakan soal yang sama dan tuliskan juga langkah pengerjaannya.

Format: Tugas9_NPM.pdf

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59