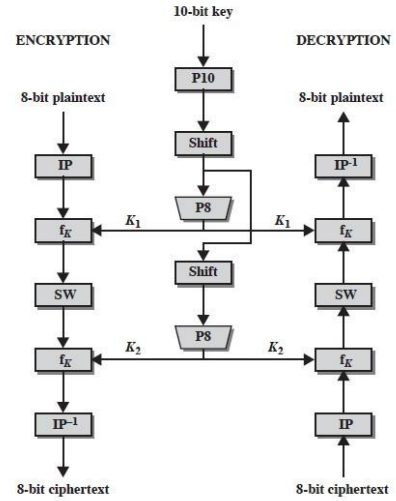
Nama: Angga Kresnabayu
Kelas: A
NPM: 140810160001

Latihan S-DES
Misalkan nama: Ragil Ananta

1. Enkripsikan huruf paling depan nama kalian dengan terlebih dahulu mengkonversikan ke ASCII (R: 82 = 01010010 – kapital). Sebagai kunci gunakan huruf terakhir nama kalian yang telah dikonversi ke ASCII dan tambahkan 01 di belakangnya (l: 108 = 01101100+01 = 0110110001 – huruf kecil)
2. Dekripsikan kembali hingga didapatkan kedua huruf tersebut (R dan l), dengan mengerjakan soal yang sama dan tuliskan juga langkah pengerjaannya.
3. Referensi program dalam bahasa pemrograman Java: **http://homepage.smc.edu/morgan_david/vpn/website-perry-sdes/all-sdes.html#SDES** in Java (dan masih banyak referensi lainnya).

Jawab




1. Enkripsi
Nama: Angga Kresnabayu
A = 65 = 0100 0001
u = 117 = 0111 0101
Plaintext: 0100 0001
Key: 01110 10101

a) Key Generation

| P10 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 3 | 5 | 2 | 7 | 4 | 10 | 1 | 9 | 8 | 6 |

| P8 | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9 |

Key: 01110 10101

Mencari nilai k1

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| K | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| P10(K) | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| Shift(P10(K)) | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| P8(Shift(P10(K)) | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | | |

Mencari nilai k2

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| K | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| P10(K) | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| Shift3(P10(K)) | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| P8(Shift3(P10(K)) | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | | |

Maka k1 = 0001 1111 dan k2 = 1110 1100

b) Inisial dan Final Permutasi

| IP | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 6 | 3 | 1 | 4 | 8 | 5 | 7 |

| $IP^{-1}$ | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 3 | 5 | 7 | 2 | 8 | 6 |

Plaintext: 0100 0001

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| P | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| IP(P) | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |

c) Fungsi Fk, SW, K

| E/P | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | 1 | 2 | 3 | 2 | 3 | 4 | 1 |

| P4 | | | |
|---|---|---|---|
| 2 | 4 | 3 | 1 |

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

1. IP(P) = 1000 0100
2. fK(L, R) = (L XOR F(R, SK), R)
   fK1 (L, R) = fK1(1000 0100) = (1000 XOR F(0100, {0001 1111}), 0100)
3. F(0100, {0001 1111}) = P4 o SBoxes o 0001 1111 XOR (E/P(0100))

4. Step

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| R | 0 | 1 | 0 | 0 | | | | |
| E/P(R) | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| K1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| E/P(R) XOR K1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| S-Boxes(E/P(R) XOR K1) | 1 | 0 | 1 | 1 | | | | |
| P4(S-Boxes(E/P(R) XOR K1) | 0 | 1 | 1 | 1 | | | | |

Perhitungan S-Boxes

a. For S0: 0011 as input: b1,b4 for row, b2,b3 for column

b. Row 01, column 01 -> output is 10 (lihat tabel)

c. For S1: 0111 as input:

d. Row 01, column 11 -> output is 11 (lihat tabel)

5. fK1 (L, R) = fK1(1000 0100) = (1000 XOR F(0100, {0001 1111}), 0100)
6. fK1 (L, R) = fK1(1000 0100) = (1000 XOR 0111, 0100)
7. fK1 (L, R) = fK1(1000 0100) = (1111, 0100)
8. L=1111 dan R=0100, SW -> R = 1111 dan L=0100

9. fK(L, R) = (L XOR F(R, SK), R)
10. fK2 (L, R) = fK2(0100, 1111) = (0100 XOR F(1111, {1110 1100}), 1111)
11. Step untuk F

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| R | 1 | 1 | 1 | 1 | | | | |
| E/P(R) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| K1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| E/P(R) XOR K1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| S-Boxes(E/P(R) XOR K1) | 1 | 1 | 0 | 0 | | | | |
| P4(S-Boxes(E/P(R) XOR K1) | 1 | 0 | 0 | 1 | | | | |

Perhitungan S-Boxes

a. For S0: 0001 as input: b1,b4 for row, b2,b3 for column

b. Row 01, column 00 -> output is 11 (lihat tabel)

c. For S1: 0011 as input:

d. Row 01, column 01 -> output is 00 (lihat tabel)

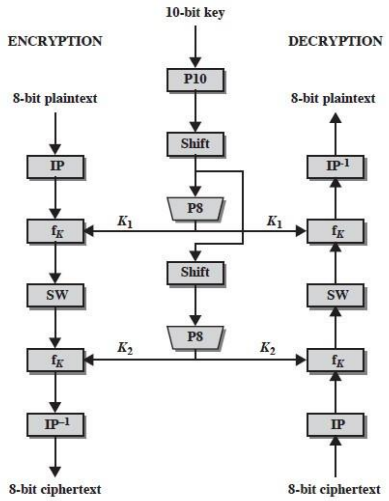
12. fK2 (L, R) = fK2(0100, 1111) = (0100 XOR F(1111, {1110 1100}), 1111)
13. fK2 (L, R) = fK2(0100, 1111) = (0100 XOR 1001, 1111)
14. fK2 (L, R) = fK2(0100, 1111) = (1101, 1111)
15. L=1101 dan R=1111, SW -> R = 1111 dan L=1101

16. Invers Permutasi

| Bit# | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| L,R | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| IP^-1(L,R) | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |

17. Maka Chippertext: 1101 1111

2. Dekripsi




Sama dengan enkripsi, maka didapat Chippertext: 1101 1111 dengan Key: 01110 10101 diperoleh Plaintext: 0100 0001 (A)

3. Sumber

http://mercury.webster.edu/aleshunas/COSC%205130/G-SDES.pdf
https://terenceli.github.io/assets/file/mimaxue/SDES.pdf
https://sandilands.info/sgordon/teaching/css322y11s2/unprotected/CSS322Y11S2H01-DES-Examples.pdf