Tugas Prak Kriptografi

21 November 2018

Nama : Patricia Joanne
NPM : 140810160065

S-DES

Soal:

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 saya : Patricia

   Huruf pertama : P (80 = 01010000) ➔ **PLAINTEXT**

   Huruf terakhir : a (97 = 01100001) ➔ **KEY**

   Key Generation

   Pengaturan ulang input dengan P10 = 0100110000

   5 bit pertama dari *1-bit left shift* = 10010

   5 bit kedua dari *1-bit left shift* = 00001

   Pengaturan ulang separuh dengan P8 = 00010010 (K1)

5 bit pertama dari *2-bit left shift* = 01010

5 bit kedua dari *2-bit left shift* = 00100

Pengaturan ulang separuh dengan P8 = 00011000 (K2)

Inisialisasi Permutasi

Didapat teks setelah inisialisasi permutasi = 10001000

4 bit pertama = 1000

4 bit kedua = 1000

Hasil setelah E/P = 01000001

E/P XOR K1 = 01010011

P4 Permutasi = 1000

L XOR F = 0000

fK (L XOR F, R) = 0000

Hasil setelah swapping = 10000000

Hasil setelah E/P = 00000000

E/P XOR K2 = 00011000

P4 Permutasi = 1111

L XOR F = 0111

fK (L XOR F, R) = 01110000

Cipher text = 10100100

2) Dekripsi

CIPHER TEXT ➔ 10100100

KEY ➔ 01100001

Key Generation

Pengaturan ulang input dengan P10 = 0100110000

5 bit pertama dari *1-bit left shift* = 10010

5 bit kedua dari *1-bit left shift* = 00001

Pengaturan ulang separuh dengan P8 = 00010010 (K1)

5 bit pertama dari *2-bit left shift* = 01010

5 bit kedua dari *2-bit left shift* = 00100

Pengaturan ulang separuh dengan P8 = 00011000 (K2)

Inisialisasi Permutasi

Didapat teks setelah inisialisasi permutasi = 01110000

4 bit pertama = 0111

4 bit kedua = 0000

Hasil setelah E/P = 00000000

E/P XOR K2 = 00011000

P4 Permutasi = 1111

L XOR F = 1000

fK (L XOR F, R) = 10000000

Hasil setelah swapping = 00001000

Hasil setelah E/P = 01000001

E/P XOR K1 = 01010011

P4 Permutasi = 1000

L XOR F = 1000

fK (L XOR F, R) = 10001000

Plain text (setelah diinverse) = 01010000