

Susulan Quiz

18 Desember 2018

Nama : Patricia Joanne

NPM : 140810160065

Enkripsi dan dekripsikan menggunakan S-DES

Key: 10 + delapan bit huruf depan nama kalian (kapital)

PT: P

JAWAB:

Huruf P → Key: 1001010000

PT: P → 01010000

Urut input key dengan P10: 0000101001

5 bit pertama setelah 1-bit left shift: 00010

5 bit kedua setelah 1-bit left shift: 10010

Urut sebagian key dengan P8 menghasilkan K1: 10010001

5 bit pertama setelah 2-bit left shift: 01000

5 bit kedua setelah 2-bit left shift: 01010

Urut sebagian key dengan P8 menghasilkan K2: 00100001

Plain text setelah diinisial permutasi: 10001000

4 bit pertama: 1000

4 bit kedua: 1000

Hasil setelah E/P: 01000001

E/P XOR K1: 11010000

P4 permutasi: 1001

L XOR F: 0001

$f_k(L \oplus F, R)$: 00011000

Hasil setelah swapping: 10000001

Hasil setelah E/P: 10000010

$E/P \oplus K_2$: 10100011

P4 permutasi: 0001

$L \oplus F$: 1001

$f_k(L \oplus F, R)$: 10010001

Cipher text setelah inverse inisial permutasi: 11000010