ENKRIPSI DENGAN ALGORITMA DES

Oleh:

Humaira Tri Acantya 5114100116  
Ilham Aulia Majid 5114100144

Kelompok F16

Kelas KIJ F

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 cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau upa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

Langkah-langkah:

1. Langkah pertama
   1. Ubah plaintext kedalam biner
   2. Ubah key kedalam biner
2. Langkah kedua: Lakukan Initial Permutation (IP) pada bit plaintext menggunakan tabel IP
3. Langkah ketiga: Generate kunci yang akan digunakanuntuk mengenkripsi plaintext dengan menggunakan tabel permutasi kompresi PC-1, pada langkah ini terjadi kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit
4. Langkah keempat: Lakukan pergeseran kiri (Left Shift)
5. Langkah kelima: Pada langkah ini, kita akan meng-ekspansi data Ri-1 32 bit menjadi Ri 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1<= i <=16 menggunakan Tabel Ekspansi (E)
6. Langkah keenam: Setiap Vektor Ai disubstitusikan kedelapan buah S-Box(Substitution Box), dimana blok pertama disubstitusikan dengan S1, blok kedua dengan S2 dan seterusnya dan menghasilkan output vektor Bi32 bit.

Referensi:

http://octarapribadi.blogspot.co.id/2012/10/contoh-enkripsi-dengan-algoritma-des.html

http://ilmu-kriptografi.blogspot.co.id/2009/05/algoritma-des-data-encryption-standart.html