DOKUMENTASI DES with OFB

KIJ F

Kelompok F02

1. I Made Fandy Aditya Wirana (5114100026)

2. Nurul Wachidah (5114100052)

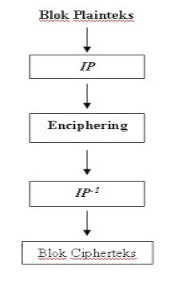
PENDAHULUAN

DES (Data Encryption Standard) adalah algoritma cipher blok yang populer karena dijadikan standard algoritma enkripsi kunci-simetri, meskipun saat ini standard tersebut telah digantikan dengan algoritma yang baru, AES, karena DES sudah dianggap tidak aman lagi. Sebenarnya DES adalah nama standard enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (Data Encryption Algorithm), namun nama DES lebih populer daripada DEA. Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel. Algoritma ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh National Security Agency (NSA) Amerika Serikat. 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.

Kami memilih implementasi DES dengan menggunakan OFB. Perbedaan mendasar OFB, yang membedakannya dengan CFB adalah input yang digunakan dalam proses enkripsi. Kalau dalam CFB, input yang digunakan adalah ciphertext yang selanjutnya dishift bersama IV, dalam OFB yang digunakan adalah output bit hasil dari proses seleksi yang kemudian dishift bersama IV yang sebelumnya. Hasil Seleksi tetap diguanakan dalam proses enkripsi Plaintext untuk mendapatkan Ciphertext.

DASAR TEORI

**DES**



Skema global dari algoritma DES adalah sebagai berikut (lihat Gambar):

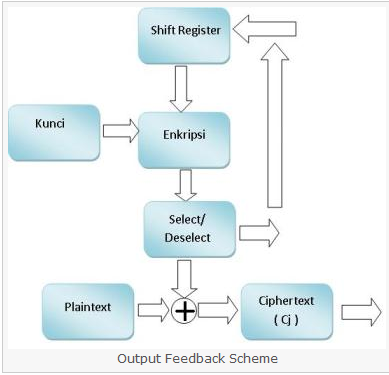
1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).

2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kaH (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1 ) menjadi blok cipherteks.

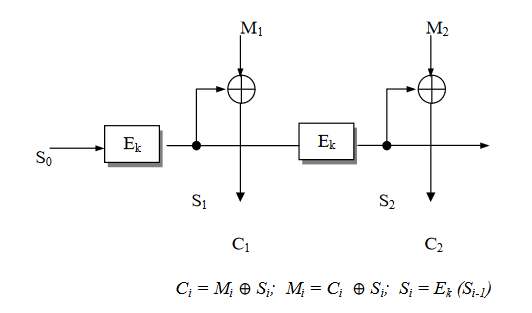
Di dalam proses enciphering, blok plainteks terbagi menjadi dua bagian, kiri (L) dan kanan R), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran i, blok R merupakan masukan untuk fungsi transformasi yang ;isebut f. Pada fungsi f, blok R dikombinasikan dengan kunci internal K,. Keluaran dai =angsi f di-XOR-kan dengan blok L untuk mendapatkan blok R yang baru. Sedangkan blok - yang baru langsung diambil dari blok R sebelumnya.

**OFB**



Mode Output Feedback (OFB mode) mirip dengan mode CFB kecuali bahwa jumlah operasi XOR dengan setiap blok plaintext dihasilkan secara

independen dari baik plaintext maupun ciphertext. Sebuah vektor inisialisasi C0 digunakan sebagai suatu “seed” untuk sebarisan blok data si, dan setiap blok data si diperoleh dari proses enkripsi terhadap blok data si-1 sebelumnya. Proses enkripsi blok plaintext diperoleh dengan melakukan operasi XOR antara blok plaintext dengan blok data yang relevan.

. 

REFERENSI

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

https://cryptobounce.wordpress.com/2008/06/19/block-cipher/

http://elib.unikom.ac.id/files/disk1/358/jbptunikompp-gdl-ridhohasil-17866-2-bab2.pdf

https://ilmukriptografi.wordpress.com/2012/04/25/kriptografi-simetrik-dasar-block-cipher/