DOKUMENTASI DES with CBC

KIJ F

Kelompok F02

1. I Made Fandy Aditya Wirana (5114100026)

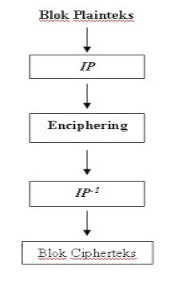
2. Nurul Wachidah (5114100052)

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 CBC. Dimana mode operasi Cipher Block Chaining (CBC) merupakan salah satu mode operasi block cipher yang menggunakan vektor inisialisasi (initialitation vector/IV) dengan ukuran tertentu (ukurannya sama dengan satu blok plaintext). Pada mode operasi ini plaintext dibagi menjadi beberapa blok, kemudian masing-masing blok dienkripsi dengan ketentuan blok plaintext pertama dienkripsi lebih dahulu. Sebelum dienkripsi, plaintext di-XOR dengan IV. Lalu, hasil XOR tersebut dienkripsi hingga menghasilkan ciphertext. Selanjutnya, ciphertext tersebut digunakan sebagai IV untuk proses penyandian blok plaintext selanjutnya. Mode operasi CBC menutupi kelemahan dari mode operasi ECB, karena pada CBC dapat menyembunyikan pola dari plaintext. Mengapa demikian? Karena sebelum dienkripsi, plaintext di-XOR dengan IV atau ciphertext sebelumnya, sehingga plaintext yang sama belum tentu menghasilkan ciphertext yang sama, kecuali jika memiliki IV/ciphertext sebelumnya yang sama. Kelemahan dari CBC adalah untuk mendekripsi ciphertext, dipengaruhi oleh ciphertext sebelumnya. Jika ada kesalahan pada ciphertext sebelumnya, maka ciphertext selanjutnya pun akan salah.

DASAR TEORI



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

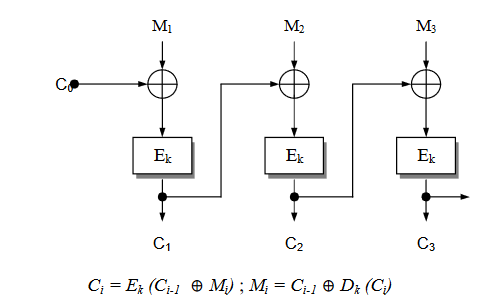
1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).

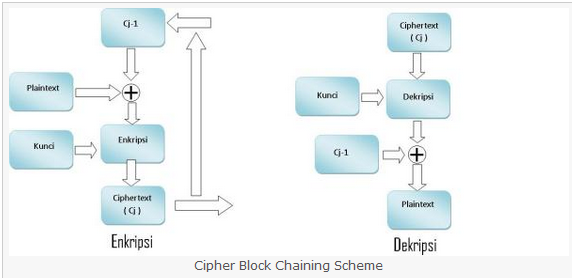
2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kaH (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

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.

Salah satu alternatif untuk mencegah munculnya blok-blok ciphertext yang sama dari blok plaintext yang sama pada satu pesan adalah dengan menggunakan mode CBC. Pada skema ini setiap blok n-bit plaintext di-XOR-kan dengan blok n-bit ciphertext sebelumnya. Kecuali blok plaintext pertama di-XOR-kan dengan suatu konstanta awal atau initialization vector (IV), sebesar n-bit. Hasil dari proses XOR tersebut yang kemudian dienkripsi. Untuk proses dekripsi, hasil dekripsi blok ciphertext di-XOR-kan dengan blok ciphertext sebelumnya untuk menghasilkan blok plaintext. Untuk blok pertama, hasil dekripsi blok ciphertext pertama di-XOR-kan dengan IV untuk menghasilkan blok plaintext pertama. Walaupun nilai IV tidak perlu dirahasiakan akan tetapi integritas dari nilai IV harus dilindungi.





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/