Algoritma Triple DES (Data Encryption Standart)

Pendahuluan

Algoritma penyandian data yang telah dijadikan standard sejak tahun 1977 adalah *Data Encryption Standard* (DES) setelah disetujui oleh *National Bureau of Standard* (NBS) dan setelah dinilai kekuatannya oleh *National Security Agency* (NSA). Algoritma DES dikembangkan di IBM di bawah kepemimpinan W.L. Tuchman pada tahun 1972. Kekuatan DES saat itu terletak pada panjang kuncinya yaitu 56-bit. Akibat perkembangan teknologi yang begitu pesat, DES, dalam beberapa hal, terbukti kurang dalam hal jaminan aspek keamanan. Perangkat keras khusus yang bertujuan untuk menentukan kunci 56-bit DES hanya dalam waktu beberapa jam sudah dapat dibangun. Dan pada tahun 1998, Electronic Frontier Foundation menggunakan suatu komputer yang dikembangkan secara khusus yang bernama DES Cracker, dalam waktu kurang dari tiga hari telah mampu untuk memecahkan DES. Beberapa pertimbangan tersebut telah manandakan bahwa diperlukan sebuah standard algoritma baru dan kunci yang lebih panjang. Setelah itu, dibuatlah beberapa pengembangan dari DES dengan cara memperbesar ruang kunci. Varian pengembangan DES yang paling dikenal adalah DES Berganda, yakni pemanfaatan DES berkali-kali untuk proses enkripsi dan dekripsinya. Double DES mempunyai kelemahan yaitu ia dapat diserang dengan algoritma yang dikenal sebagai meet-in-the-middle-attack, yang pertama kali ditemukan oleh Diffie dan Hellman. Sebagai bentuk pencegahan terhadap serangan tersebut, maka digunakanlah tiga kali langkah DES. Bentuk tersebut dinamakan sebagai Triple DES.

Beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok Triple DES di antaranya adalah *Electronic Code Book* (ECB), *Cipher Block Chaining* (CBC), *Cipher Feedback* (CFB), dan *Output Feedback* (OFB).

Bentuk Umum Triple DES

Konsep Triple DES sebenarnya sama dengan DES, namun terdapat beberapa

pengembangan, yaitu:

Bentuk umum TDES (mode EEE):

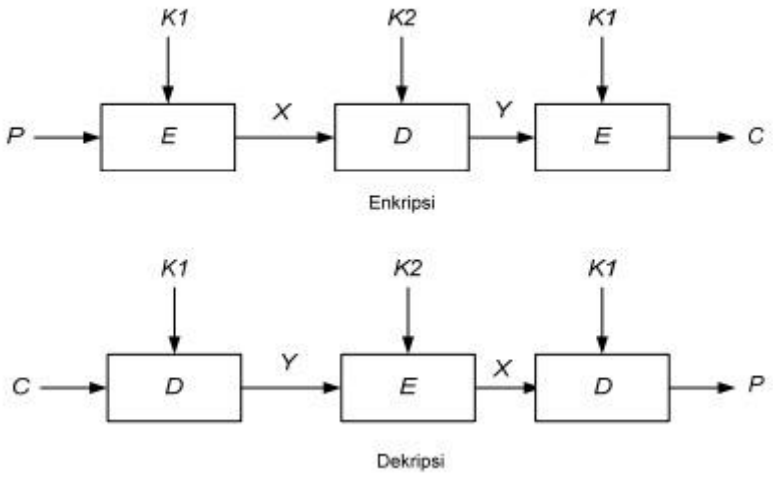
Enkripsi: C = EK3(EK2(EK1 (P)))

Dekripsi: P = DK1(DK2 (DK3 (C)))

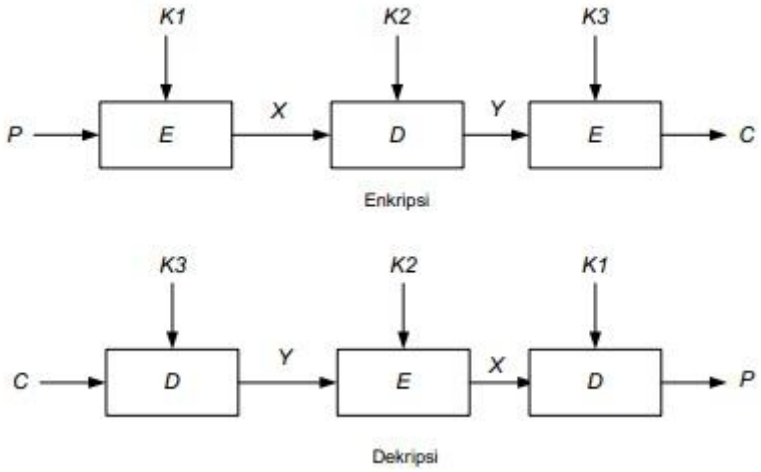
Untuk menyederhanakan TDES, maka langkah di tengah diganti dengan D (mode EDE). Ada dua versi TDES dengan mode EDE:

- Menggunakan 2 kunci
- Menggunakan 3 kunci

Berikut merupakan skema Triple DES dengan 2 kunci :



Dan di bawah ini adalah skeme Triple DES dengan 3 kunci :



Kriptoanalis Pada Triple DES

Kriptoanalisis pada Triple DES dapat menggunakan key search attack dan exploit known (atau chosen) pairs of plainteks dan cipherteks. Pengukuran keberhasilan dan kompleksitas dari serangan kriptoanalisis adalah sebagai berikut :

a. Jumlah pasangan known plainteks-cipherteks.
b. Storage space yang dibutuhkan untuk serangan.
c. Jumlah single encryption.
d. Jumlah keseluruhan operasi/step untuk serngan.

Cara yang paling ampuh untuk serangan Triple DES adalah dengan menggunakan MITM. Jika pasangan plainteks dan cipherteks (p,c) diberikan, dapat dilakukan proses sebagai berikut :

- Hitung semua nilai bN = D3N(c), N{0,1}k, dan simpan pasangan (bN,N) dalam tabel, dengan indeks bN.
- Hitung semua nilai bLM = E2M(E1L(p)) dengan L,M {0,1}k, dan cari (bL,M,N) di tabel pasangan (bN,N) yang telah dihitung sebelumnya.
- Tes seluruh triple (L,M,N) dengan bLM = bN sampai hanya tinggal satu dri triple yang ada.

REFERENSI

Adeputra Anugrah. 2009. *Studi & Implementasi Algoritma Triple DES.*

Desutha. 2009. *Ringkasan Algoritma DES.* http://www.scribd.com/doc/48763620/des. di akses 4 mei 2012.

Tropsoft. 2008. *Triple DES Encryption.* http://www.tropsoft.com/strongenc/des3.htm. di akses 4 mei 2012.