ANALISA ALGORITMA BLOCK CIPHER DALAM PENYANDIAN DES DAN PENGEMBANGANNYA

Stefanus Astrianto N – NIM : 13504107

Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if114107@students.if.itb.ac.id

Abstract - *Makalah ini membahas tentang studi terhadap salah satu algoritma kriptografi block cipher, yaitu DES (Data Encryption Standard). DES adalah salah satu metode penyandian dengan sistem* block cipher. *Yaitu sistem penyandian yang pengacakannya dilakukan secara blok demi blok dengan blok input (teks asli) 64 bit dan menghasilkan output (teks sandi) yang juga per blok 64 bit, algoritma yang digunakan adalah kunci simetris dengan panjang kunci 56 bit.*

Algoritma ini termasuk algoritma penyandian simetris, dimana untuk proses enkripsi dan dekripsi pesan menggunakan kunci yang sama. Jadi, walaupun seorang kriptografer mengerti dengan baik algoritma yang digunakan untuk menyandikan pesan tersebut, tapi kalau tidak tahu kunci yang digunakan, maka tidak akan dapat mendekripsi pesan tersebut. Dalam makalah ini juga akan dijelaskan sejarah DES, beberapa kelemahan dan kelebihan algoritma DES, serta perbandingannya dengan beberapa algoritma pengembangannya seperti Triple DES dan AES.

Kata kunci*: Data Encryption Standard*, *cipher block*, enkripsi, dekripsi, Lucifer, DES, Triple DES, IBM, kriptografi, Jaringan Feistel.

1. Pendahuluan

Masalah keamanan merupakan salah satu aspek penting dari sebuah system informasi. Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data, ataupun informasi adalah enkripsi. Disini enkripsi dapat diartikan sebagai kode atau chiper . Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah chipper menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari suatu pesan asli (plaintext) menjadi cryptogram yang tidak di mengerti. Karena sistem chipper merupakan suatu sistem yang telah siap untuk di outomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

Pertengahan tahun 1973, Pemerintah Amerika Serikat (AS) melalui *National Bureau of Standards* (NBS) mengumumkan kebutuhan akan suatu algoritma sandi yang akan digunakan sebagai standar untuk melindungi kerahasiaan dan keutuhan data-data penting baik yang sedang ditransmisikan maupun yang disimpan.

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.

Sampai pertengahan tahun 1974 tidak ada satupun algoritma sandi yang diusulkan. Hingga akhirnya pada tanggal 6 Agustus 1974, algoritma sandi yang didesain oleh IBM yang bernama sistem sandi Lucifer ditawarkan kepada NBS. Kemudian setelah dilakukan evaluasi dan modifikasi dengan bantuan *National Security Agency* (NSA), pada tanggal 15 Juli 1977 NBS menetapkan algaritma Lucifer yang telah dimodifikasi tersebut dengan nama baru *Data Encryption Standard* atau lebih populer dengan sebutan sistem sandi DES.

Setelah ditetapkan sebagai standar untuk melindungi data dan informasi baik yang ditransmisikan maupun yang disimpan, sistem sandi DES dengan cepat digunakan secara internasional pada hampir

diberbagai aplikasi yang membutuhkan penyandian pada saat operasionalnya.

Tercatat penggunaan sistem sandi DES terbesar saat itu adalah pada industri perbankan disamping pemerintahan dan militer. Hal ini mengingat pada institusi tersebut data / informasi yang ditansmisikan dan disimpan banyak yang merupakan data penting yang sensitif dan bersifat rahasia.

2. Cara Kerja Algoritma DES

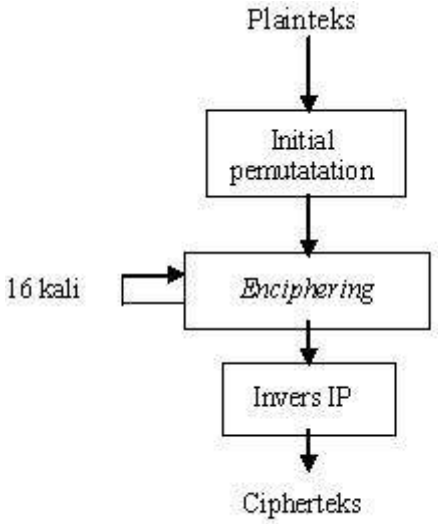
Sebagai sistem sandi modern yang berbasiskan peralatan elektronik, DES beroperasi dalam bentuk bit yang berupa angka binari 0 dan 1, yang berkelompok dengan masing-masing kelompok terdiri dari 4 bit membentuk bilangan heksadesimal atau bilangan berbasis 16.

Binari : 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

Heksadesimal : 0 1 2 3 4 5 6 7 8 9 A B C D E F

DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

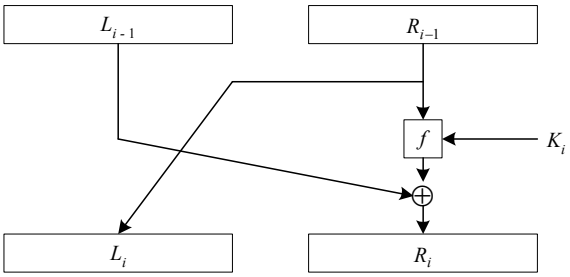
Algoritma dasarnya adalah pertama-tama dengan mempermutasikan dengan matriks permutasi awal(*initial permutation*), kemudian mencipherkannya dengan sebuah fungsi F sebanyak 16 putaran, dan terakhir adalah dengan mempermutasikannya lagi dengan invers dari matriks yang dipakai sebelumnya (*invers initial permutation*)



Gambar 1 Skema Dasar DES

Pada setiap tahapnya, sebuah blok yang terdiri 64 bit dibagi menjadi 2 bagian, yaitu bagian kiri(L) dan bagian kanan(R). Bagian R disimpan untuk menjadi bagian L untuk tahap selanjutnya, kemudian R dimasukkan ke dalam fungsi F dengan menggunakan kunci internal K yang dibangkitkan pada setiap tahapnya. Hasilnyadi-XOR-kan dengan L kemudian disimpan untuk menjadi R tahap selanjutnya.

$$L' = R$$
$$R' = L \oplus f(R,K)$$

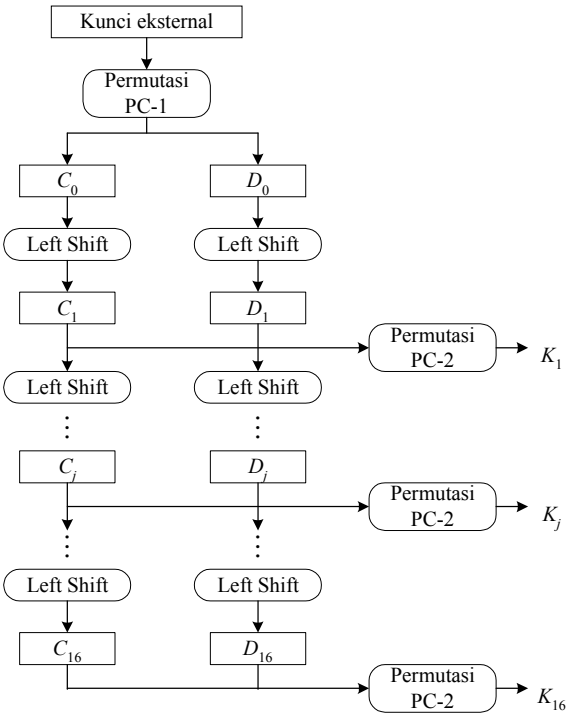


Gambar 2 Jaringan Feistel

Proses di atas disebut sebagai Jaringan Feistel, dimana proses ini dilakukan berulang sebanyak 16 kali. Proses harus dilakukan sebanyak itu untuk mencegah pemecahan kode melalui known-plaintext-attack.

Seperti apa yang telah disebutkan sebelumnya, DES menggunakan 56 bit kunci untuk melakukan enkripsi dan dekripsi blok masukan. Kunci internal

dibangkitkan dari kunci eksternal yang diberikan oleh user. Kunci eksternal tersebut panjangnya 64 bit (8 byte) atau 8 karakter. Namun tiap bit ke-8 (parity bits) dari 8 byte kunci tersebut diabaikan. Oleh karena itu, hanya ada 56 bit kunci yang digunakan (effective bits). Permutasi yang dilakukan pada bit-bit ini disebut dengan permuted choice 1. Permuted choice 1 ini mengubah posisi bit-bit pada kunci eksternal dan mengurangi bit kunci eksternal yang awalnya berjumlah 64 bit menjadi 56 bit dengan cara menghilangkan parity bits.

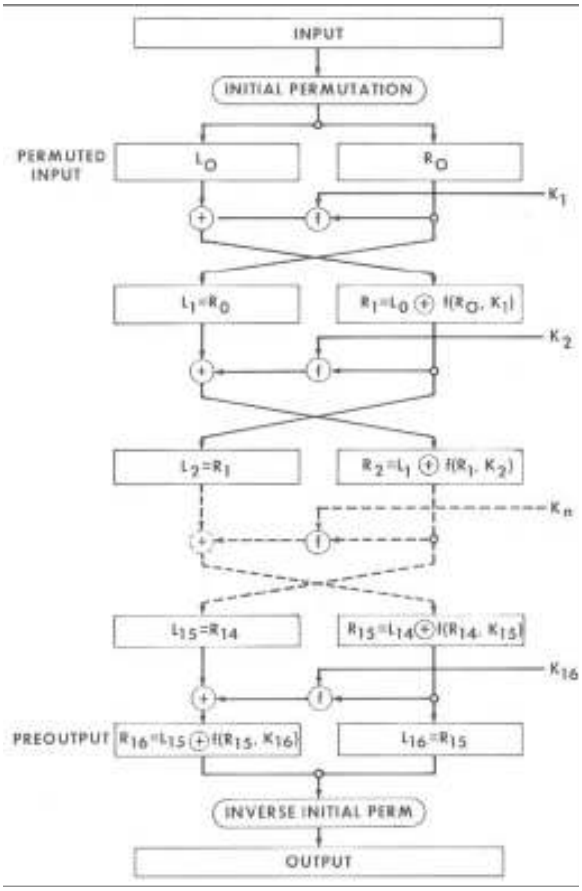


Gambar 3 Pembangkitan Kunci Internal

Kunci internal yang diperoleh dibagi menjadi 2 bagian, kiri (C) dan kanan (D), yang masing-masing panjangnya 28 bit. D terdiri dari bit pada posisi ke-0 hingga ke-27, sedangkan C terdiri dari bit pada posisi ke-28 hingga ke-55. Kedua bagian digeser ke kiri (left shift) sepanjang 1 atau 2 bit bergantung pada tiap putaran. Setelah pergeseran bit, dilakukan permutasi (*permuted choice 2*) pada hasil pergeseran bit dari kedua bagian tersebut untuk memperoleh kunci internal pada tiap putaran, yang selanjutnya disebut dengan subkey.

Proses dekripsinya dilakukan dengan menggunakan algoritma yang sama, tetapi menggunakan susunan kunci yang dibalik urutannya.

.



Gambar 4 Skema Keseluruhan DES

3. Analisa Algoritma DES

Sebelum distandarkan, DES (saat itu masih bernama Lucifer) menggunakan algoritma dengan panjang kunci 128 bit, namun oleh Pemerintah AS panjang kunci DES dibatasi hanya diperbolehkan 56 bit saja dengan maksud agar NSA (*National Security Agency*) dapat memonitor informasi yang disandikan dengan sistem DES tersebut. Selain menentukan panjang kunci, NSA juga mengubah S-Box (*Substitution Box*) nya sehinga walaupun S-Box tersebut diubah secara acak, NSA tetap dapat membongkar sistem sandi DES tersebut.

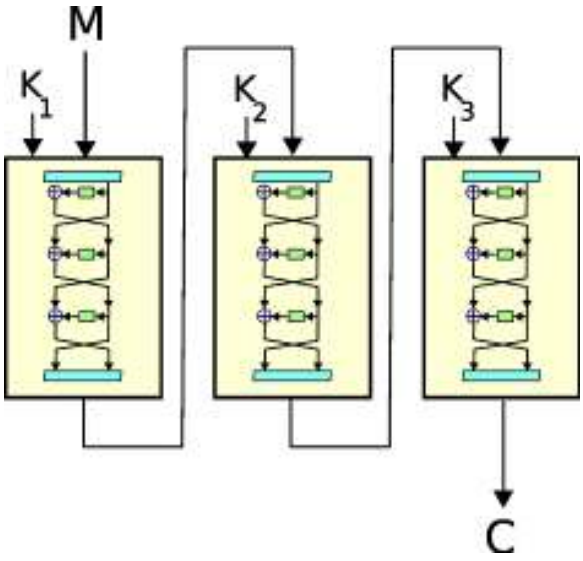
Saat ini satu-satunya cara yang diketahui untuk mendobrak sandi DES adalah dengan mencoba satu per satu berbagai kombinasi kunci (istilahnya: brute force attack). Di samping itu, proses enkripsi yang dilakukan sebanyak 16 putaran juga menyulitkan untuk proses kriptanalis. Karena itu keamanan dari DES banyak bergantung dari ukuran kunci yang

digunakan (dalam bit). Ukuran tersebut menentukan jumlah kombinasi kunci yang mungkin. DES menggunakan ukuran kunci 56 bit sehingga total banyaknya kombinasi kunci yang mungkin adalah 2^{56}. Jumlah ini sangat besar. Untuk membongkar sandi tersebut dengan menggunakan PC Pentium yang berkemampuan mengerjakan 200 juta operasi per detik kita masih membutuhkan 5 tahun. Dengan mesin yang lebih baik orang bisa melakukannya lebih cepat, tetapi biayanya juga menjadi mahal. Ini membuat usaha pembongkaran seperti itu menjadi tidak ekonomis.

Ternyata timbul masalah setelah DES resmi dijadikan algoritma standar nasional. Masalah pertama adalah panjang kunci DES yang hanya 56-bit sehingga amat sangat rawan dan riskan serta berbahaya , terhadap *brute-force attack.*Masalah kedua adalah struktur DES pada bagian *substitution-box* (S-box) yang diubah menurut saran dari NSA. Desain *substitution-box* dirahasiakan oleh NSA sehingga kita tidak mengetahui kemungkinan adanya kelemahan-kelemahan pada DES yang sengaja disembunyikan oleh NSA. Dan juga muncul kecurigaan bahwa NSA mampu membongkar cypher tanpa harus memiliki key-nya karena menurut para "pakar" kriptografi, DES sudah didesain secara cermat sehingga kalau S-box ini diubah secara acak maka sangat mungkin DES justru lebih mudah "dijebol" meskipun DES cukup kebal terhadap serangan *differential cryptanalysis* maupun *linier cryptanalysis.*

Seperti kata peribahasa "Karena susu setitik rusak iman sebelanga" ,.Di dunia ini tak ada ciptaan manusia yang sempurna.Pada tahun 1998, 70 ribu komputer di internet berhasil menjebol satu kunci DES dengan waktu sekitar 96 hari.Bahkan pada tahun 1999 berhasil dibobol dalam waktu kurang dari 22 hari.Pada tanggal 16 juni 1998 ada sebuah kelompok yang menamakan dirinya Electronic Frontier Foundation (EFF) telah berhasil memecahkan DES dalam waktu 4-5 hari menggunakan komputer yang dilengkapi dengan Integrated Circuit Chip DES Cracker.Di akhir tragedi ini, DES dianggap sudah tak aman lagi sehingga ia dicampakkan begitu saja dan digantikan oleh AES (Anvanced Encryption Standard).

Salah satu solusi untuk memperbaiki algoritma ini adalah dengan menggunakan panjang kunci yang lebih dari 64, karena sudah terbukti bahwa kunci tersebut dapat dipecahkan hanya dalam beberapa hari. Algoritma Triple DES menggunakan kunci 2x56 atau 112bit.



Gambar 5 Algoritma Triple DES

Triple DES adalah pengembangan dari algoritma DES. Pada dasarnya algoritma yang digunakan adalah sama, hanya dikembangkan dengan menggunakan dua kunci yang berukuran 56 bit. Kunci pertama digunakan untuk enkripsi pesan dan kunci kedua digunakan untuk dekripsi pesan. Perkembangan yang lain adalah Triple DES ini melakukan enkripsi dengan implementasi algoritma DES sebanyak 3 kali.

Varian lain Algoritma DES adalah AES (*Advanced Encryption Standard*)Algoritma AES didesain oleh dua orang Belgia, Vincent Rijmen dan Joan Daemen. Di-publish pertama kali pada tahun 1998 dan tergolong block chiper. AES dikenal juga bernama Rijndael. AES ini merupakan salah satu dari sekian banyak desain yang lolos seleksi dan akhirnya diadopsi oleh NIST (National Institute of Standards dan Technology) menjadi standard untuk Amerika pada tahun 2001. AES dikenal sebagai algoritma enkripsi yang cukup cepat baik jalan di perangkat lunak maupun perangkat keras. Selain itu AES relatif lebih mudah untuk diimplementasikan dan lebih sedikit memakan resource (sumber daya) memori. Ukuran block chiper pada AES adalah 128 bit dengan panjang key bervariasi yaitu 128, 192 atau 256 bit. Sampai saat ini (2004) AES masih dianggap cukup aman untuk melindungi informasi atau data pemerintah Amerika yang sifatnya non-classified. Pada tahun 2003 pemerintah Amerika akhirnya mengumumkan bahwa AES bisa juga digunakan untuk melindungi informasi atau data yang sifatnya classified.

Walaupun berbasis algoritma Rijndael, AES tidak sama persis seperti Rijndael. Rijndael mendukung semakin besar ukuran block chiper dan panjang key. AES hanya memiliki ukuran block chiper yang sudah pasti (fixed) sebesar 128 bit. Walaupun dipandang aman, banyak yang menguji keamanan dari algoritma AES ini. Pada tahun 2002 melalui suatu proses pengujian yang sifatnya teoritis ditemukan bahwa AES mungkin untuk dijebol atau dipecahkan. Metode attack ini dinamakan "XSL attack". Metode ini diumumkan oleh Nicolas Courtois dan Josef Pieprzyk namun metode inipun juga masih spekulatif dan belum bisa dibuktikan saat ini (2004).

4. Daftar Pustaka

[1] *http://www.cert.or.id/~budi/courses/ec7010/2003/report-avon.pdf*

[2] *http://hadiwibowo.wordpress.com/2007/06/27/sistem-sandi-des-data-encryption-standard/*

[3] *http://safitri1404.wordpress.com/2007/06/10/algoritma-des-1/*

[4] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[5] Schneier, Bruce. (1996). Applied Cryptography 2nd. John Wiley & Sons.

[6] *http://203.130.205.68/dosen/aji/computer_security/bab_2.pdf*