Studi dan Analisis Dua Jenis Algoritma Block Cipher: DES dan RC5

Zakiy Firdaus Alfikri - 13508042
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
zakiy_f_a@yahoo.co.id

***Abstrak*—Algoritma yang sering diaplikasikan dalam mengenkripsi suatu file di tahun-tahun terakhir ini adalah algoritma yang termasuk ke dalam algoritma block cipher. Ada banyak jenis algoritma block cipher yang ada, di antaranya adalah DES, RC5, 3DES, GOST, AES, SAFER, LOKI, IDEA, dan masih banyak lagi.**

Block cipher merupakan suatu jenis algoritma kriptografi yang sistem penyandiannya dilakukan per blok dari keseluruhan data atau pesan yang ingin dienkripsi. Block cipher berbeda dengan stream cipher yang penyandiannya dilakukan per karakter data atau pesan.

DES merupakan salah satu yang memakai algoritma yang berjenis block cipher. DES (Data Encryption Standart) adalah suatu standar algoritma kriptografi yang memakai algoritma block cipher dengan sandi block kunci simetrik dengan ukuran block 64 bit dan ukuran kunci 56-bit.

RC5 juga merupakan salah satu jenis algoritma block cipher. RC5 (Rivest Cipher 5) adalah algoritma block cipher dengan ukuran block yang bervariasi, 32, 64, atau 128 bit dan ukuran kunci yang juga bervariasi, antara 0 sampai 2040 bit dan juga perulangan yang bervariasi antara 0 sampai 255.

DES dan RC5 merupakan algoritma yang berbeda. Keduanya mampunyai kelebihan dan kekurangan masing-masing. Pada makalah ini akan dibahas perbandingan kedua jenis algoritma enkripsi ini.

***Index Terms*—block cipher, DES, RC5, enkripsi.**

I. PENDAHULUAN

Data dan pesan yang penting biasanya mempunyai nilai privasi yang tinggi dan isinya hanya boleh diketahui oleh orang-orang yang berkepentingan saja. Oleh karena itu harus ada suatu metode yang bisa digunakan untuk menjaga kerahasiaan data dan pesan tersebut. Ada sebuah metode yang bisa dipakai untuk mengatasi masalah ini yaitu kriptografi.

Kriptografi adalah sebuah ilmu dan seni untuk menjaga keamanan pesan dengan cara menyandikan data dan pesan ke dalam bentuk yang tidak dimengerti lagi makna aslinya. Ada banyak jenis algoritma kriptografi yang bisa dipakai, mulai dari algoritma kriptografi klasik yang sederhana sampai algoritma kriptografi modern yang sulit dipecahkan.

Salah satu algoritma modern yang sering diaplikasikan adalah jenis algoritma cipher block. Algoritma ini menyandikan data dan pesan perblok-blok data atau pesan yang ingin dienkripsi. Ada banyak jenis algoritma yang berjenis algoritma kriptografi cipher block, di antaranya adalah DES, RC5, 3DES, GOST, AES, LOKI, SAFER, IDEA, dan masih banyak lagi.

Dalam makalah ini akan dibahas dua buah algoritma modern yang berjenis algoritma cipher block, yaitu DES dan RC5.

Ada perbedaan di antara kedua jenis algoritma kriptografi tersebut baik dari algoritma yang dipakai sendiri, proses pengenkripsian, cara kriptanalisis, dan juga kekuatan cipher teks yang dihasilkan.

II. DES DAN RC5

DES adalah singkatan dari Data Encryption Standart adalah sebuah standar untuk suatu algoritma kriptografi. Algoritma yang sebenarnya dimaksud adalah DEA, yang merupakan singkatan dari Data Encryption Algorithm.

Algoritma ini merupakan hasil pengembangan dari algoritma Lucifer yang dirancang oleh Horst Feistel. Algoritma pada DES dikembangkan oleh sekelompok orang pada IBM yang salah satunya adalah Horst Feistel, pencipta Lucifer. DES merupakan algoritma standar kriptografi di Amerika yang disetujui oleh NBS (National Bureau of Standart setelah kekuatan dari algoritma yang dipakai diakui oleh NSA (National Security Agency)

Amerika Serikat.

RC5 adalah singkatan dari Rivest Cipher 5 yang dirancang oleh Ronald. RC5 dikembangkan untuk RSA Security pada tahun 1994. Algoritma RC5 merupakan algoritma cipher block yang sederhana yang bisa mengenkripsi ukuran blok yang bervariasi, 32, 64, atau 128 bit. Pengembangan RC5 yaitu RC6 merupakan kandidat dari Advanced Encryption Standart.

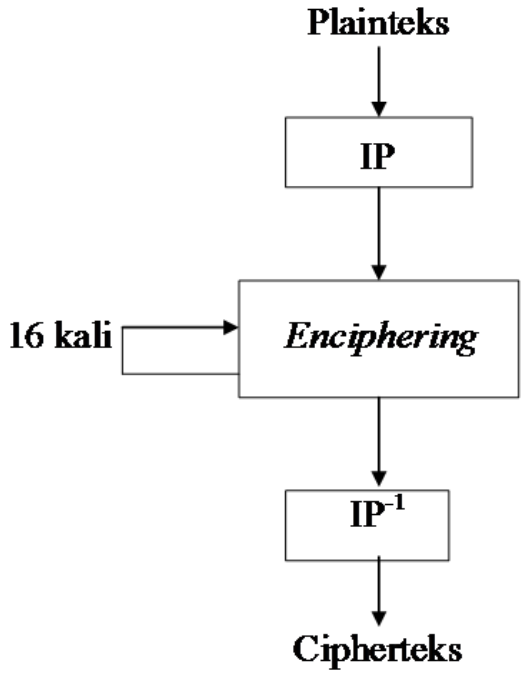
III. ALGORITMA PADA DES DAN RC5

Algoritma DES dan RC5 sama-sama merupakan algoritma yang mengaplikasikan block cipher, tapi ada perbedaan algoritma yang dipakai oleh keduanya.

A. Algoritma pada DES

Pada algoritma yang dipakai dalam DES, enkripsi dilakukan sebanyak 16 putaran yang setiap putarannya menggunakan kunci internal yang berbeda. Kunci-kunci internal ini dibangkitkan dari kunci eksternal. Setiap blok akan mengalami permutasi awal, 16 kali putaran enkripsi, dan inversi permutasi awal.

Berikut ini adalah skema global dari algoritma yang digunakan dalam DES.



Gambar 1. Skema global DES

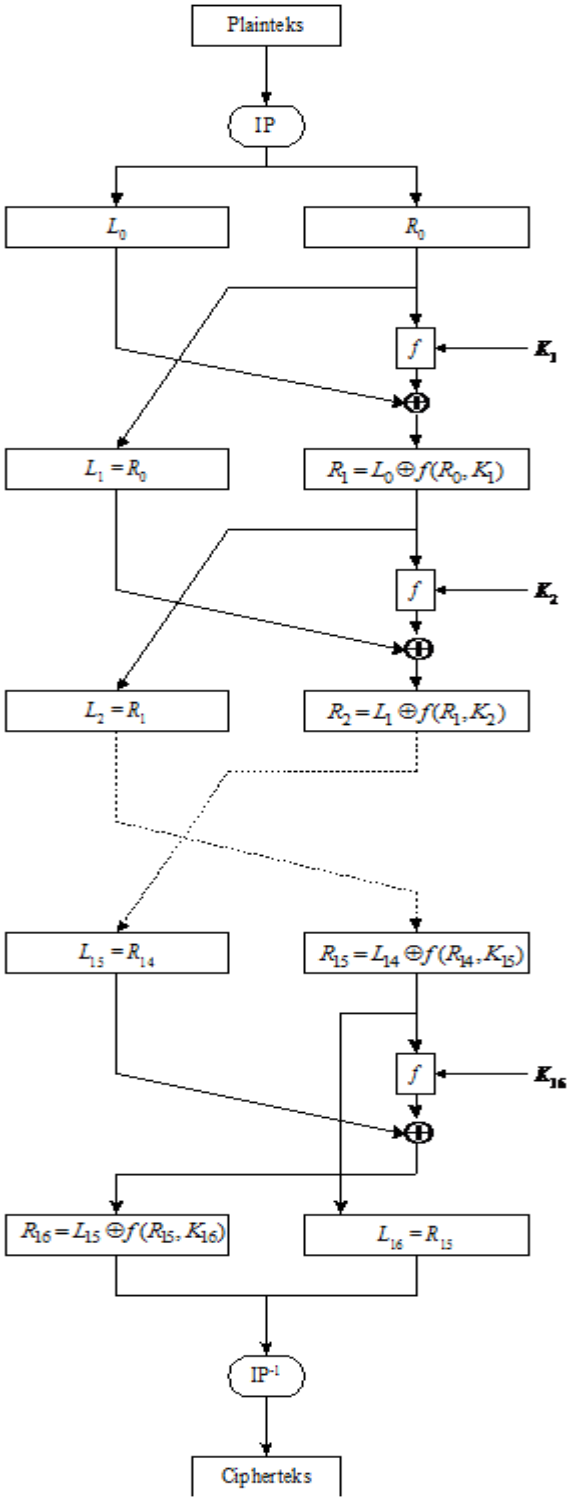
Bisa dilihat pada skema global di atas plain teks akan dikenai permutasi awal lalu dikenai enciphering sebanyak 16 kali. Setelah itu hasil dari 16 kali enciphering tersebut akan dikenai inversi dari permutasi awal yang akan menghasilkan cipher teks yang diinginkan.

Di dalam enciphering diimplementasikan jaringan Feistel seimbang. Jaringan Feistel adalah struktur simetri yang digunakan untuk membangun sebuah algoritma block cipher. Jaringan Feistel merupakan iterasi cipher dengan fungsi internal di dalamnya, *f*, yang sering disebut round function.

Dalam proses enciphering yang ditunjukkan pada skema global DES, plain teks yang sudah dikenai permutasi awal akan dibagi menjadi dua bagian blok yaitu L0 dan R0. R0 akan dikenai fungsi *f* yang merupakan fungsi internal dalam jaringan Feistel. Fungsi internal ini juga akan melibatkan kunci K1. Hasilnya akan dikenai operasi XOR dengan L0. Hasil operasi XOR akan menjadi R1. Dan L1 bernilai R0.

Setelah itu proses di atas akan diulang untuk L1 dan R1. Proses akan terus berulang sampai 16 putaran (sampai mendapat L16 dan R16). Setelah 16 putaran L16 dan R16 akan dikenai operasi inversi dari permutasi awal untuk mendapatkan cipher teks yang diinginkan.

Berikut ini adalah skema dari algoritma enkripsi seperti sudah dijelaskan sebelumnya.



Gambar 2. Skema algoritma enkripsi pada DES

B. Algoritma pada RC5

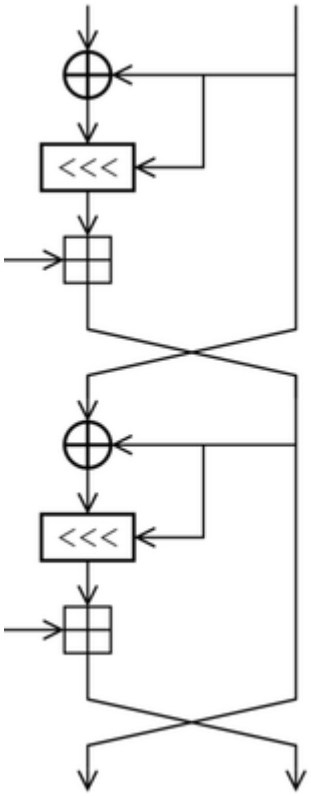
Pada algoritma RC5 juga dilakukan pengulangan sama seperti pada DES, akan tetapi pengulangan yang dilakukan pada algoritma RC5 lebih bervariasi, bisa dilakukan 1 sampai 255 pengulangan. Walaupun begitu disarankan untuk melakukan sebanyak 12 kali pengulangan.

Selain itu ukuran block yang akan dienkripsi juga bervariasi, 32, 64, atau 128 bit. Disarankan untuk menggunakan block dengan panjang ukuran 64 bit. Begitu pun dengan kunci yang digunkan. Kunci yang digunakan panjangnya juga bervariasi mulai dari 0 sampai 2040 bit, yang disarankan mneggunakan kunci dengan ukuran 128 bit.

Operasi-operasi yang digunakan pada algoritma RC5 merupakan operasi-operasi yang sederhana. Operasi-operasi yang digunakan adalah operasi modular addition, XOR, dan cyclic rotation.

Struktur yang digunakan adalah struktur jaringan yang mirip jaringan Feistel (Feistel-like network).

Berikut ini bisa dilihat skema dari algoritma enkripsi pada RC5 untuk satu pengulangan, terdiri dari dua buah setengah pengulangan.



Gambar 3. Skema RC5 untuk satu pengulangan

Bisa dilihat pada skema RC5 untuk satu kali pengulangan (dua kali setengah pengulangan) di atas, pada awal blok yang akan dienkripsi dibagi menjadi dua bagian sama seperti pada DES. Blok bagian kiri akan di-XOR-kan dengan blok bagian kanan. Setelah itu hasilnya akan dikenai left rotation dengan blok bagian kanan, simbol <<< menandakan left rotation. Hasil yang diperoleh akan dikenai modular addition dengan kunci yang sesuai dengan perulangan yang sedang dilakukan.

Proses ini berulang sekali lagi. Dengan blok bagian kiri adalah blok bagian kanan sebelumnya, dan blok bagian kanan adalah hasil yang diperoleh pada proses sebelumnya.

Bisa dilihat dari skema algoritma RC5 bahwa algoritma yang digunakan cukup sederhana dan pendek. Berikut ini adalah pseudo code dari algoritma enkripsi dan dekripsi RC5.

Pseudo code enkripsi dengan RC5 bisa dilihat sebagai berikut.

```
A <- A + S[0]
B <- B + S[1]
for i<-1 to r do
     A <- ((A XOR B) <<< B) + S[2*i]
     B <- ((B XOR A) <<< A) + S[2*i+1]
```

Lalu pseudo code untuk dekripsi dengan RC5 bisa dilihat sebagai berikut.

```
for i<-r downto 1 do
     B <- ((B – S[2*i+1]) >>> A) XOR A
     A <- ((A - S[2*i]) >>> B) + XOR B
B <- B - S[1]
A <- A - S[0]
```

Pada algoritma RC5, kunci yang dimasukkan diekspansi untuk mendapatkan sub-sub kunci untuk tiap pengulangan. Proses ekspansi kunci ini melibatkan dua buah variabel temporari yang menggunakan dua buah bilangan konstan sebagai berikut.

$P_w = Odd((e - 2)2^w)$
$Q_w = Odd((\Phi - 1)2^w)$

di mana,

$e = 2.718281828459...$
$\Phi = 1.618033988749...$

Lalu akan dicari kunci S dengan pseudo code sebagai berikut.

```
S[0] <- Pw
for i<-1 to t-1 do
     S[i] <- S[i-1] + Qw
```

Kunci-kunci yang dihasilkan akan di-mixing sesuai pseudo code sebagi berikut.

```
for i<- b-1 downto 0 do
     L[i/u] <- (L[i/u] <<< 8) + K[i]


I <- j <- 0
A <- B <- 0
do 3*max(t,c)times
     A <- S[i] <- (S[i] + A + B) <<< 3
     B <- L[j] <- (L[j] + A + B) <<<
(A + B)
     i <- (i + 1) mod(t)
     j <- (j + 1) mod(c)
```

IV. KRIPTANALISIS

Kriptanalisis adalah ilmu dan teknik yang digunakan untuk memecahkan suatu hasil enkripsi. Pada kebanyakan algoritma kriptografi yang beredar ada metode-metode tertentu yang bisa digunakan untuk memecahkan cipher teks hasil enkripsinya.

Begitu pun pada DES dan RC5, kedu algoritma kriptografi ini memiliki celah yang memungkinkan seorang kriptanalis untuk memecahkan cipher teks yang dihasilkan kedua algoritma tersebut dan mendapatkan plain teks yang dibutuhkan.

A. Kriptanalisis pada DES

Walaupun sudah pernah diakui sebagai algoritma enkripsi standar oleh NSA, DES memiliki celah yang memungkinkan untuk dilakukan pemecahan cipher teks menjadi plain teks yang asli.

Metode yang digunakan untuk melakukan kripatanalisis DES adalah brute force attack pada kunci yang digunakan. Selain itu ada beberapa serangan yang bisa digunakan untuk memecahkan DES yaitu differential cryptanalysis, linear cryptanalysis, dan improved Davies' attack.

Pada kriptanalisis dengan menggunakan brute force, yaitu dengan memasukkan kunci-kunci yang dimungkinkan. Karena ukuran kunci yang dipakai 56 bit maka akan ada dua pangkat 56 kemungkinan kunci yang dihasilkan.

Kriptanalisis DES pernah dilombakan untuk menguji kekuatan DES dengan hadiah sebanyak 10.000 dollar Amerika. Hadiah itu berhasil dimenangkan oleh sekelompok kriptanalis yang

memanfaatkan ribuan komputer melalui internet.

Lalu pada tahun 1998 dibangun sebuah mesin DES-cracker yang dibuat oleh Electronic Frontier Foundation yang menghabiskan dana sebesar 250.000 US dollar.

Setelah itu juga dibuat mesin bernama COPACOBANA pada tahun 2006 yang juga berhasil memecahkan cipher teks yang dienkripsi dengan DES.

Selain brute force juga ada teknik lain yang bisa digunakan. Pertama adalah differential cryptanalisis, yang ditemukan oleh Eli Biham dan Adi Shamir pada akhir 1980an. Teknik ini menggunakan dua pangkat 47 plain teks yang sudah ditentukan.

Lalu ada linear cryptanalysis yang ditemukan oleh Mitsuru Matsui. Teknik ini membutuhkan dua pangkat 43 plain teks yang sudah ditentukan.

Selain brute force, differential cryptanalysis dan linear cryptanalysis juag ada teknik improved Davies's attack. Teknik ini memang ditujukan khusus untuk mengkriptanlisis DES yang ditemukan oleh Donald Davies. Teknik ini menggunakan dua pangkat 50 plain teks yang sudah ditentukan.

B. Kriptanalisis pada RC5

Sama seperti DES, RC5 juga mempunyai celah yang dimungkinkan untuk dilakukan kriptanalisis. RC5 dengan sedikit pengulangan akan sangat rentan terhadap serangan differential attack.

RC5 dengan pengulangan sebanyak 12 kali dengan blok ukuran 64 bit rentan terhadap serangan differential attack dengan menggunakan dua pangkat 44 plain teks yang sudah ditentukan.

Untuk mengatasi hal itu maka perlu dibuat RC5 dengan pengulangan yang lebih banyak. Pengulangan sebanyak 18 sampai 20 kali cukup untuk memperkuat cipher teks yang dihasilkan.

RSA Security sebagai pemegang paten atas RC5 mengadakan lomba memecahkan cipher teks yang dibentuk dari algoritma RC5 ini. Dengan menggunakan brute force dan distributed computing, salah satu peserta lomba akan bisa memecahkan cipher teks itu setelah 90 tahun.

V. PERBANDINGAN DAN KESIMPULAN

DES maupun RC5 merupakan algoritma-algoritma yang sama-sama mengimplementasikan block cipher. Pada rancangan algoritma keduanya juga sama-sama memanfaatkan jaringan Feistel, RC5 memakai jaringan Feistel-like. Berdasarkan algoritma dan proses yang dilakukan keduanya hampir sama. Akan tetapi RC5 mempunyain ukuran blok, kunci, dan jumlah perulangan yang bervariasi.

Jika dibandingkan berdasarkan kekuatan cipher teks yang dihasilkan, sampai sekarang yang memiliki performansi lebih baik adalah RC5. DES sudah bisa dipecahkan dengan menggunakan berbagai teknik kriptanalisis yang sudah dijelaskan sebelumnya. RC5 mempunyai kelebihan di bagian ini jika dibandingkan DES, akan tetapi pengulangan yang dilakukan oleh RC5 harus banyak (lebih dari 18 kali pengulangan) jika mau menghasilkan cipher teks yang kuat.

REFERENCES

1. Menezes, A. 1996. *Handbook of Applied Cryptography*. CRC Press.
2. people.csail.mit.edu/rivest/Rivest-**rc5**rev.pdf
3. csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
4. http://orlingrabbe.com/des.htm.
5. http://people.csail.mit.edu/rivest/Rivest-rc5.pdf

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 April 2011

ttd

Zakiy Firdaus Alfikri
13508042