PS3-DX: Peningkatan Keamanan dengan Modifikasi Cipher Triple DES

M. Rafli Zamzami - 13519067 , Jusuf Junior Athala - 13519174
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail:
13519067@std.stei.itb.ac.id , 13519174@std.stei.itb.ac.id

PS3-DX merupakan proposal blok cipher yang didasarkan pada cipher DES, khususnya dari cipher Triple-DES. Cipher ini menggunakan Triple DES dengan tambahan melakukan shift bitwise dengan permutasi acak dan menggunakan key whitening.

Keywords—Cipher Blok; Triple DES; key whitening; shift bitwise acak

I. Introduction

Saat ini, pesan dapat dengan mudah ditransfer dari satu tempat ke tempat lain. Namun, terdapat pesan yang bersifat sensitif dan tidak boleh diketahui isinya oleh pihak yang tidak berhak untuk mengetahui pesan tersebut. Untuk menjaga isi pesan tersebut, dibuat sebuah sistem yang akan mengenkripsi pesan tersebut sehingga pesan tidak mudah terbaca.

Salah satu metode untuk enkripsi adalah cipher Data Encryption Standard (DES) [4]. Namun, DES yang menggunakan kunci 56 bit sudah dianggap tidak aman. Jumlah kunci yang kecil menyebabkan DES mudah diserang oleh exhaustive search [1]. Oleh sebab itu, berbagai metode telah ditemukan yang menggunakan cipher DES sebagai dasarnya dan mengurangi kelemahan yang dimiliki cipher DES. Cipher-cipher tersebut adalah Double DES, Triple DES [2], dan DES-X [3].

Pada makalah ini, kami membuat sebuah cipher PS3-DX yang merupakan kombinasi dari Triple DES dan DES-X dengan diberi tambahan metode keamanan lainnya. Cipher ini akan menerima sebuah pesan akan diubah menjadi sedemikian rupa agar dapat dibagi menjadi blok blok yang berukuran 128 bit. Kunci dari pengguna yang akan digunakan berukuran 128 bit. Jumlah putaran yang akan dilakukan pada enkripsi DES adalah 16 putaran.

II. Dasar Teori

Cipher DES dimulai dengan mengenkripsi pesan yang berukuran 64 bit atau sama dengan 16 angka hexadecimal. DES akan menggunakan kunci dengan panjang 64 bit. Namun setiap kunci bit ke-8 tidak digunakan, sehingga ukuran kunci yang digunakan secara efektif adalah 56 bit. Pesan yang akan dienkripsi akan melalui sejumlah putaran. Sebelum memasuki putaran, pesan dibagi menjadi dua bagian pesan dengan ukuran masing-masing 32 bit. Pada saat memasuki putaran, pesan akan melalui jaringan Feistel. Jaringan Feistel ini akan menyebabkan operasi dekripsi bersifat simetris dari operasi enkripsi pesan. Masing-masing bagian pesan akan mengalami proses shift dan XOR dari fungsi key schedule.

Pada DES-X yang merupakan modifikasi cipher DES, yaitu DES-X akan melakukan key whitening atau melakukan XOR pada pesan sebelum enkripsi DES dimulai. Key whitening juga dilakukan ketika enkripsi DES selesai.

Cara kerja dari PS3-DX adalah pesan yang akan dienkripsi akan melalui tahap key whitening pada awal enkripsi dan akhir enkripsi yang merupakan metode yang digunakan pada DES-X. Kemudian, pesan akan melalui proses enkripsi DES sebanyak tiga kali yang merupakan konsep Triple DES. Metode tambahan selain penggunaan DES-X dan Triple DES adalah ketika terjadi operasi shift bitwise, banyaknya bit yang di-shift akan diatur pada tabel permutasi acak. Ini akan menyebabkan operasi shift bitwise tidak linear.

III. Rancangan Block Cipher

A. Inisialiasi

Cipher PS3-DX akan menggunakan basis cipher DES, sehingga akan memerlukan inisialisasi P-Box dan S-Box. PS3-DX juga memanfaatkan tabel permutasi yang akan digunakan sebagai tabel lookup untuk operasi shift bitwise acak permutasi. Kunci masukan yang berukuran 128 bit akan digunakan sebagai kunci cipher pada operasi DES dan kunci untuk proses key whitening. Kunci masukan akan dilakukan shift menggunakan tabel permutasi empat kali sehingga menghasilkan dua kunci cipher yang berbeda untuk operasi DES dan dua kunci whitening yang berbeda.

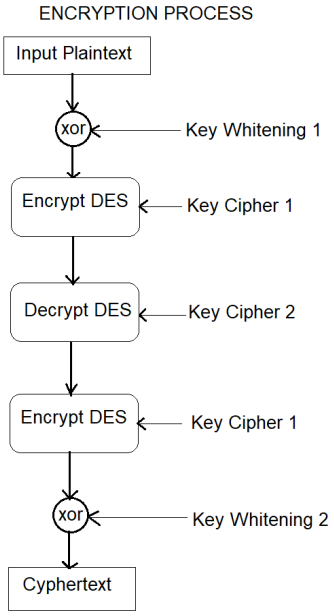
B. Kombinasi Key Whitening (DES-X) & Triple DES

Pesan akan melalui proses key whitening, yaitu pesan akan dilakukan operasi XOR terhadap key whitening pertama ketika sebelum memulai operasi enkripsi Triple DES dan dilakukan operasi XOR terhadap key whitening kedua ketika operasi enkripsi Triple DES selesai.

Setelah pesan dilakukan key whitening pertama, pesan akan melalui enkripsi Triple DES. Triple DES dimulai dengan enkripsi DES dengan kunci cipher DES pertama. Hasil dari enkripsi DES pertama akan dilakukan operasi dekripsi DES dengan menggunakan kunci cipher DES kedua. Hasil dari dekripsi kedua ini kemudian akan dilanjutkan dengan operasi enkripsi menggunakan kunci cipher pertama. Ini akan

menghasilkan cipherteks yang kemudian akan dilakukan key whitening kedua. Hasil dari key whitening kedua inilah yang akan menjadi hasil akhir ciphertext.

Berikut adalah diagram untuk kombinasi key whitening & enkripsi Triple DES



Gambar 1. Diagram kombinasi DES-X dan Triple DES

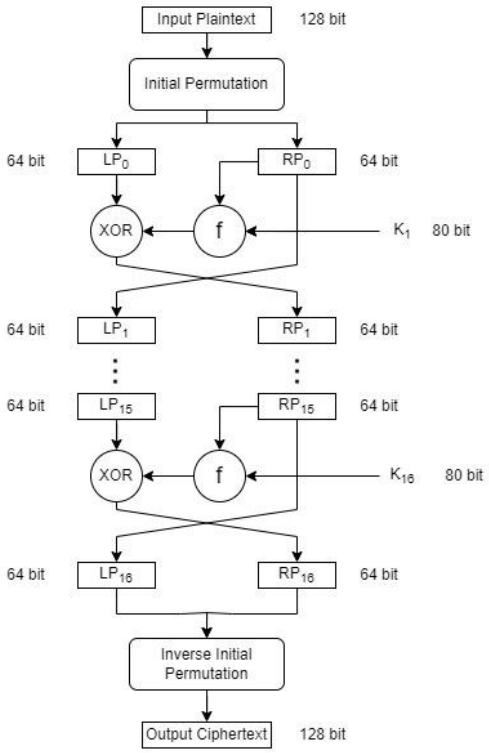
C. Jaringan Feistel untuk Enkripsi DES

Proses enkripsi DES akan dimulai dengan pesan diacak melalui permutasi awal sehingga urutan bit berubah yang menggunakan matriks P-Box yang sudah diinisialisasi. Kemudian pesan akan dipisah menjadi dua bagian berukuran sama.

Kedua bagian pesan ini akan mengalami putaran enkripsi. Bagian kedua atau bagian kanan pesan akan digunakan untuk putaran berikutnya sebagai pesan bagian kiri. Bagian kanan pesan ini juga akan digunakan fungsi F yang akan menerima kunci internal hasil pembangkitan key cipher. Hasil dari fungsi F ini akan dilakukan operasi XOR pada bagian pesan pertama atau bagian kiri pesan. Hasil XOR ini akan menjadi bagian kanan pesan untuk putaran berikutnya. Putaran ini akan dilakukan sebanyak 16 kali.

Hasil dari 16 putaran enkripsi akan dilakukan inversi permutasi yang menggunakan matriks invers dari P-Box. Hasil inversi permutasi ini adalah hasil ciphertext.

Berikut adalah jaringan feistel untuk enkripsi DES.

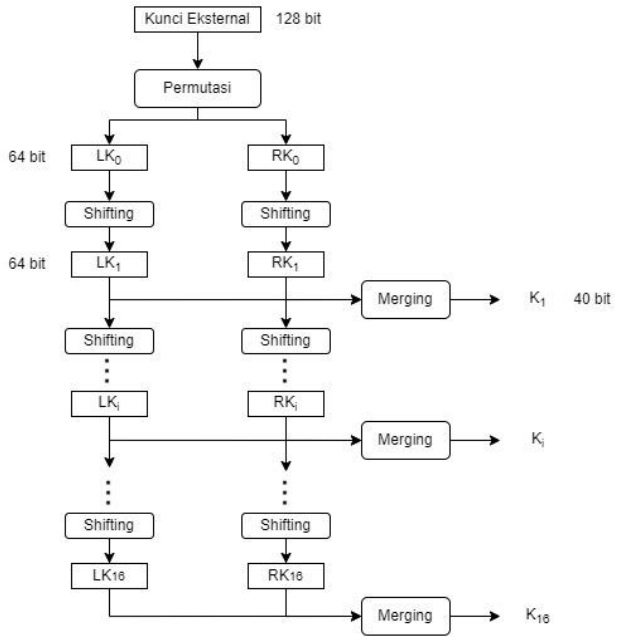


Gambar 2. Diagram jaringan Feistel untuk DES

D. Pembangkitan Kunci Internal

Dalam enkripsi DES, terdapat fungsi F yang membutuhkan kunci internal yang merupakan hasil pembangkitan dari key cipher. Kunci external atau kunci yang diterima dari masukan user berukuran 128 bit akan mengalami permutasi. Kemudian kunci dibagi menjadi 2 bagian berukuran sama. Masing-masing bagian akan dilakukan shift secara permutasi acak dan kemudian akan digabung kembali sehingga menghasilkan sebuah kunci internal. Shifting secara permutasi acak akan dilakukan sebanyak 16 putaran, sehingga total kunci internal yang akan diciptakan adalah sebanyak 16 kunci internal.

Berikut adalah diagram pembangkitan kunci internal untuk enkripsi DES.

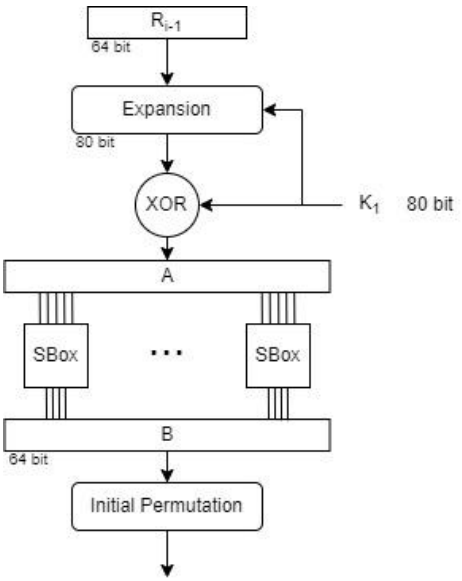


Gambar 3. Diagram pembangkitan kunci internal

E. Fungsi F

Pada enkripsi DES, bagian pesan kanan akan dilakukan fungsi F. Pesan bagian kanan yang berukuran 64 bit akan mengalami ekspansi sehingga ukuran nya menjadi 80 bit. Kemudian, pesan yang berukuran 80 bit akan dilakukan operasi XOR dengan key hasil pembangkitan dari key cipher. Hasil XOR tersebut akan dilakukan substitusi berdasarkan S-Box yang telah diinisialisasi. Kemudian hasil penggabungan semua substitusi S-Box akan mengalami permutasi untuk mengacak urutan hasil S-Box.

Berikut adalah diagram fungsi F.



Gambar 4. Diagram Fungsi F

F. Shift menggunakan tabel permutasi

Untuk setiap operasi shift yang terjadi, sebuah angka acak akan diambil dari sebuah tabel permutasi yang telah diinisialisasi. Ini menyebabkan jumlah shift yang terjadi pada setiap putaran di enkripsi DES bersifat nonlinear.

IV. Eksperimen dan Pembahasan Hasil

A. Waktu Enkripsi

PS3-DX menggunakan Triple DES dengan tambahan operasi XOR dengan key whitening. Oleh sebab itu, jika dibandingkan dengan Triple DES, PS3-DX akan memakan waktu yang lebih lama.

B. Analisis Efek Longsoran

Pada PS3-DX, efek longsoran akan terjadi ketika 1 bit pada ciphertext hasil enkripsi mengalami perubahan. Contohnya adalah sebagai berikut.

Ciphertext semula :

1101111110011000000100101100111101101100011000001100111100111001100100101110000001000011010011101001000010011111111101010101111101

Hasil Dekripsi semula:

0123456789ABCDEF0123456789ABCDEF

Ciphertext dengan perubahan 1 bit pada bit ke-3 dari 0 menjadi 1:

1111111110011000000100101100111101101100011000001100111100111001100100101110000001000011010011101001000010011111111101010101111101

Hasil Dekripsi setelah perubahan 1 bit:

E67EE6324C6C1214B2368A0118F8417A

Efek longsoran ini membuktikan bahwa PS3-DX sulit untuk diserang melalui percobaan menebak kunci.

C. Analisis Ruang Kunci

Ruang kunci untuk cipher PS3-DX dapat dihitung sebagai berikut. Awal mula kunci input dari pengguna adalah 128 bit, sehingga ruang kunci berukuran 2^128. Namun, PS3-DX menggunakan basis cipher DES sehingga untuk key setiap bit ke-8 tidak akan digunakan sehingga hanya akan ada 2^112 bit ruang kunci.

V. Kesimpulan dan Saran

Terdapat banyak metode enkripsi pesan. Salah satunya adalah DES. Namun, DES memiliki kelemahan yaitu jumlah kunci yang kecil. Kelemahan ini dapat diatasi dengan metode Triple DES dan DES-X. Dengan menggabungkan enkripsi DES tiga kali atau disebut juga Triple DES dan menggunakan prinsip key whitening yang digunakan DES-X dan perubahan operasi shift menjadi operasi shift berdasarkan permutasi, tingkat keamanan enkripsi dapat diperkuat dan pesan enkripsi akan lebih sulit untuk diserang. Namun, penggunaan enkripsi DES berulang sebanyak tiga kali akan memakan waktu dan

resource, sehingga masih dapat dikembangkan cara yang lebih efisien.

Daftar Referensi

[1] W. Diffie and M. Hellman, "Exhaustive cryptanalysis of the NBS Data Encryption Standard." Computer, vol.10, no.6, 74-84 , Juni 1977

[2] R. Merkle and M. Hellman, “On the Security of Multiple Encryption”, Communications of the ACM, vol. 24, no. 7, pp. 465–467, July 1981.

[3] J. Kilian and P. Rogaway, “How to protect DES against exhaustive key search”, Advances in Cryptology - Crypto '96, Springer-Verlag (1996), pp. 252–267.

[4] W. Tuchman , "A brief history of the data encryption standard", Internet besieged: countering cyberspace scofflaws. ACM Press/Addison-Wesley Publishing Co. New York, NY, USA. pp. 275–280, 1997