PERBANDINGAN METODE MODIFIKASI 3DES DENGAN METODE 3DES

Emmy Apulina Br. Bangun [#1], Gamaliel Natawijaya Setiawan [#3]

[#] *Departemen Teknik Informatika*

Fakultas Teknik, Institut Teknologi Harapan Bangsa

JL. Dipatiukur No. 80 – 82, Bandung 40122

emmy@ithb.ac.id

Abstrak— Kriptografi dapat dibedakan menjadi 2 yaitu kriptografi dengan menggunakan kunci simetri dan kriptografi dengan menggunakan kunci asimetri. Contoh kriptografi kunci simetri adalah 3DES (Triple Data Encryption Standard) dan kriptografi kunci asimetri adalah RSA. Pada aplikasi ini penulis memodifikasi metode 3DES (Triple Data Encryption Standard) sehingga pengamanan terhadap text dapat lebih aman dibandingkan 3DES. Modifikasi metode 3DES yang dilakukan menghasilkan ciphertext yang lebih panjang dan ada penambahan proses pada proses enkripsi dan dekripsinya.

Kata kunci— Cryptography, Modifikasi 3DES

Abstract— Cryptography can be divided into 2 key cryptography using symmetric and asymmetric key cryptography using. Examples of symmetric key cryptography is 3DES (Triple Data Encryption Standard) method and asymmetric key cryptography is RSA method. In this application, the authors modified the method of 3DES (Triple Data Encryption Standard) so that the security of the text can be more secure than 3DES method. Triple DES modification method produces cipher text that is longer than 3 DES and there are additional processes on the encryption and decryption process.

Keywords— Cryptography, Modification 3DES, 3DES symmetric key

I. PENDAHULUAN

Meningkatnya kebutuhan informasi secara cepat mendorong meningkatnya kemajuan teknologi informasi secara pesat pula, termasuk didalamnya teknologi pengiriman pesan. Saat ini, jarak yang jauh yang memisahkan antara pengirim dan penerima pesan bukan merupakan suatu halangan lagi dalam hal pengiriman pesan. Pesan dengan mudah dan cepat dapat dikirim dengan dukungan teknologi internet, intranet, dan lain-lain.

Untuk pengamanan pesan, banyak metode-metode kriptografi yang dapat diterapkan dalam sesi komunikasi antara pengirim dan penerima pesan.

Tujuan yang ingin dicapai dalam penelitian ini adalah bagaimana membuat modifikasi terhadap salah satu metode enkripsi yang telah ada yaitu 3DES sehingga keamanan data dapat lebih terjamin.

II. KRIPTOGRAFI

Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu "Crypto" berarti "secret" (rahasia) dan "graphy" berarti "writing" (tulisan). Terdapat 2 jenis algoritma dalam kriptografi, yaitu algoritma kriptografi Simetris dan Asimetris.Algoritma kriptografi simetris adalah algoritma yang menggunakan kunci yang sama baik untuk proses enkripsi maupun untuk proses dekripsi. Sedangkan algoritma kriptografi asimetris, kunci yang digunakan untuk proses enkripsi berlainan dengan kunci untuk melakukan proses dekripsi. Untuk jenis algoritma yang terakhir, kunci-kunci yang digunakan disebut dengan kunci public dan kunci private.

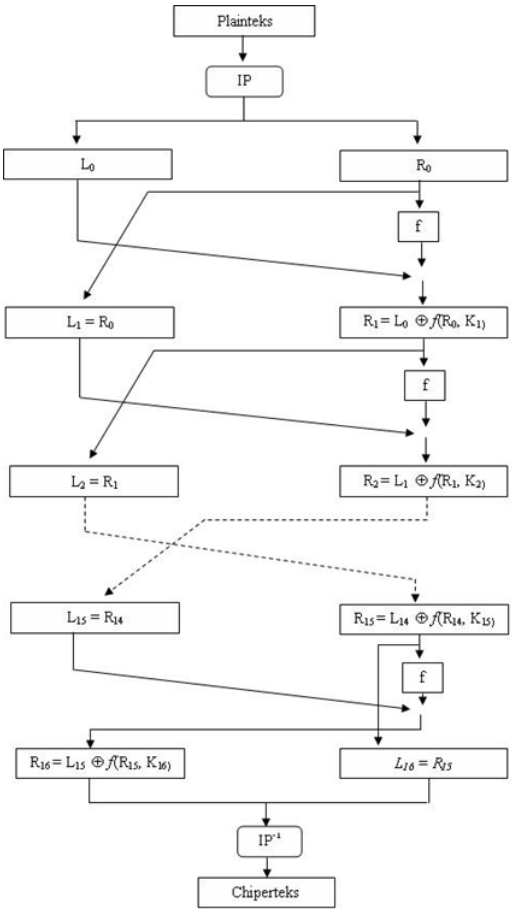
Jenis algoritma simetris yang sering digunakan untuk mengamankan pesan dalam melakukan sesi komunikasi diantaranya DES dan 3 DES.

A. DES

Pada Algoritma DES, teks dienkrip dalam blok-blok 64 bit dengan menggunakan 56 bit kunci internal. Kunci internal berasal dari kunci eksternal yang panjangnya 64 bit. Blok-blok teks input tersebut ditransformasikan kedalam blok-blok output 64 bit juga dengan menggunakan beberapa tahapan.

Tiga tahapan besar dalam DES yaitu:

1) Plaintext yang berukuran 64 bit dipermutasi dengan matriks permutasi awal.
2) Hasil permutasi awal kemudian di-enciphering-sebanyak 16 kali (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.

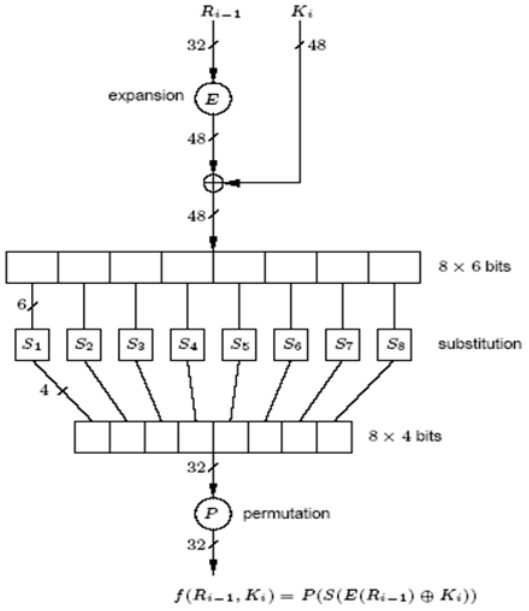


Gambar 2.1. Proses iterasi enkripsi DES

Setiap putaran dalam DES terdiri atas 6 proses. Berikut adalah proses-proses yang terjadi diputaran pertama.

1) Ekpansi R_0
2) Pencarian bit-bit K_1
3) $E(R_0)$ XOR K_1
4) Mengsubtitusi hasil dari proses 3 kedalam S- Box Output
5) $f(R_0,K_1)$
6) $L_2 = R_1$

Gambaran tahap-tahapan didalam satu putaran tersebut dapat dilihat pada gambar 2.2.



Gambar 2.2. Proses-proses setiap putaran DES

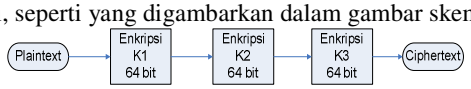
B. 3DES

Metoda 3 DES menggunakan DES sebanyak 3 kali. Bentuk sederhana perhitungan untuk enkripsi dan dekripsi 3 DES adalah :

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

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

Bentuk ini dikenal dengan mode EEE karena untuk memperoleh cipherteks dilakukan proses enkripsi sebanyak tiga kali, seperti yang digambarkan dalam gambar skema 2.3.



Gambar 2.3. Enkripsi EEE 3DES

Sedangkan skema untuk dekripsinya digambarkan pada gambar2.4 .

Gambar 2.4. Dekripsi EEE 3DES

Bentuk perhitungan 3DES lainnya yang menggunakan 3 buah kunci yang berbeda adalah :

Enkripsi : $C = E_{K3}(D_{K2}(E_{K1}(P)))$

Dekripsi : $P = D_{K1}(E_{K2}(D_{K3}(C)))$

Untuk skema enkripsi dan dekripsinya terlihat seperti gambar dibawah ini.

Gambar 2.5. Enkripsi EDE 3 DES

Gambar : Dekripsi EDE 3 DES

Selain menggunakan 3 kunci, metode 3 DES juga dapat dibuat varian lainnya dengan menggunakan hanya 2 kunci. Proses perhitungannya yaitu sebagai berikut :

Enkripsi : $C = E_{K1}(D_{K2}(E_{K1}(P)))$

Dekripsi : $P = D_{K1}(E_{K2}(D_{K1}(C)))$

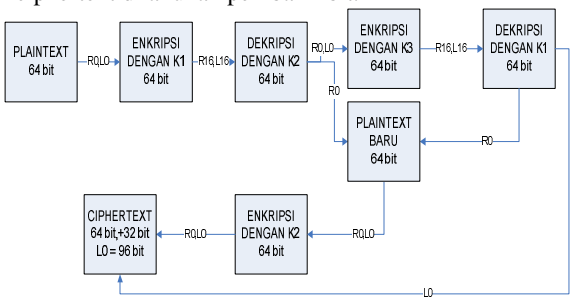
III. MODIFIKASI 3 DES

Dalam memodifikasi 3 DES digunakan 3 buah kunci yang berbeda, yaitu K1, K2, dan K3. Bentuk perhitungan M-3DES, yaitu :

Ciphertext = $(((((E_{K1}(P))D_{K2})E_{K3})D_{K1})E_{K2})$

Langkah-langkah proses enkripsi M-3DES :

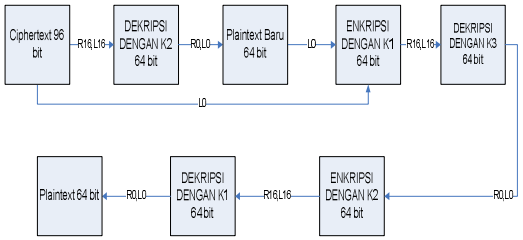
1) Plaintext yang berukuran 64 bit di enkripsi dengan kunci pertama yang menghasilkan R16 dan L16
2) Kemudian di dekripsi dengan kunci kedua yang menghasilkan R0 dan L0
3) Kemudian di enkripsi dengan kunci ketiga yang menghasilkan R16 dan L16
4) Kemudian di dekripsi dengan kunci pertama yang menghasilkan R0 dan L0
5) R0 yang berukuran 32 bit dari dekripsi kunci kedua dan R0 yang berukuran 32 bit dari dekripsi kunci pertama dijadikan plaintext baru dimana menjadi R0 dan L0, kemudian plaintext tersebut di enkripsi dengan kunci kedua sehingga menghasilkan R16 dan L16 lalu di permutasi inverse, kemudian L0 yang berukuran 32 bit dari dekripsi kunci pertama ditambahkan setalah hasil permutasi inverse tersebut dan sebelum menjadi ciphertext dilakukan pembalik bit.



Gambar 3.1. Skema Enkripsi M-3DES

Langkah-langkah proses dekripsi M-3DES :

1) Ciphertext yang berukuran 96 bit dilakukan pembalik bit
2) 64 bit pertama dari ciphertext di dekripsi dengan K2 sehingga menghasilkan R0 dan L0
3) 32 bit sisa dari ciphertext dan L0 yang menghasilkan 64 bit di enkripsi dengan kunci pertama yang menghasilakn R16 dan L16
4) Kemudian di dekripsi dengan kunci ketiga yang menghasilkan R0 dan L0
5) Kemudian di enkripsi dengan kunci kedua yang menghasilkan R0 dan L0 yang kemudian di lakukan permutasi awal sehingga menghasilkan plaintext yang berukuran 64 bit.



Gambar 3.2. Skema dekripsi 3 DES

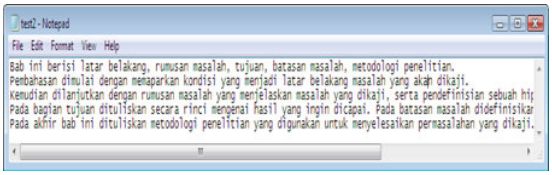
Bentuk perhitungan dekripsi M-3DES :

Plaintext = $(((((D_{K2}(C))E_{K1})D_{K3})E_{K2})D_{K1})$

IV. PENGUJIAN

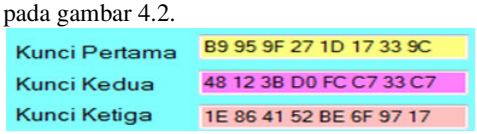
Pengujian diperlukan untuk melihat seberapa besar efek pemodifikasian DES terhadap metode 3 DES sebelumnya. Berikut salah satu hasil pengujian dari pengujian-pengujian yang telah dilakukan.

Teks yang akan dilakukan pengujian terhadap metode M-3 DES dan 3 DES adalah teks yang diperlihatkan pada gambar 4.1.



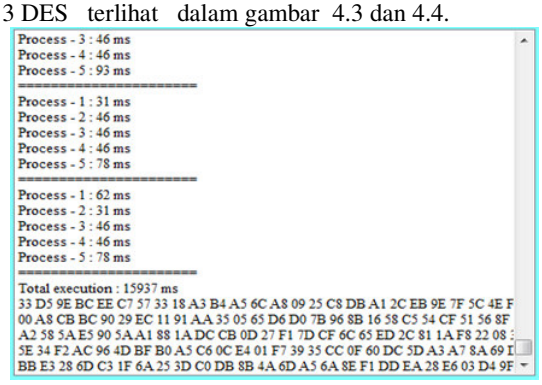
Gambar 4.1. Teks yang akan diuji

Sedangkan kunci-kunci hasil generate sistem yang digunakan untuk enkripsi dan dekripsi adalah seperti yang terlihat pada gambar 4.2.

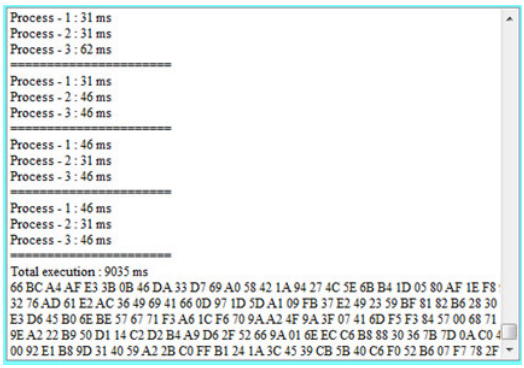


Gambar 4.2. Kunci-kunci enkripsi dan dekripsi M-3DES dan 3 DES

Sebagian tahapan proses enkripsi untuk metode M- 3 DES dan 3 DES terlihat dalam gambar 4.3 dan 4.4.

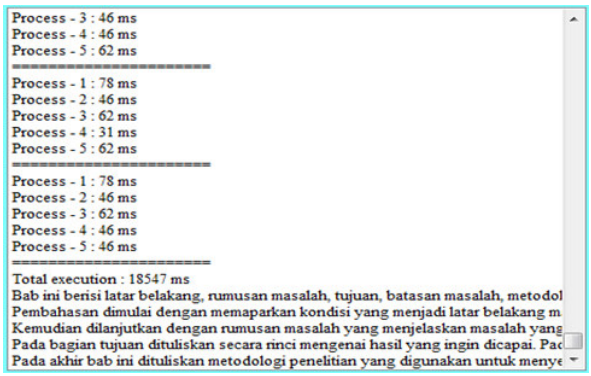


Gambar 4.3. Tahapan Enkripsi dengan Metode M-3DES

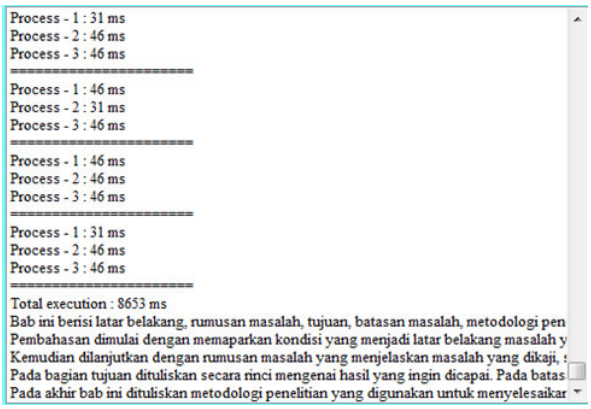


Gambar 4.4.Tahapan Enkripsi dengan Metode 3 DES

Untuk membuktikan apakah cipherteks yang dihasilkan oleh proses enkripsi dapat dikembalikan ke plainteks asli maka dilakukan proses dekripsi seperti yang terlihat dalam gambar 4.5 dan 4.6.



Gambar 4.5.Tahapan Dekripsi dengan Metode M-3DES



Gambar 4.6.Tahapan Dekripsi dengan Metode 3DES

V. KESIMPULAN

Kesimpulan yang di peroleh selama penelitian dilakukan adalah sebagai berikut :

1) Proses yang terdapat didalam modifikasi 3 DES lebih banyak dan rumit, sehingga waktu yang dibutuhkan untuk proses enkripsi juga lebih banyak.
2) Waktu yang dibutuhkan dalam melakukan dekripsi pada hasil modifikasi 3 DES lebih lama, karena proses yang harus diselesaikan juga lebih banyak dibandingkan dengan 3 DES .
3) Waktu yang dibutuhkan untuk enkripsi berbeda dengan waktu yang dibutuhkan untuk dekripsi pada masing-masing metode.

REFERENSI

[1] Bangun,Emmy Apulina Br dan Setiawan,Gamaliel Natawijaya, Enkripsi dan Dekripsi dengan Metode Modifikasi Data Encryption Standard pada Text,ITHB,2010.

[2] Ariyus, Dony, Kriptografi Keamanan Data Dan Komunikasi, Graha Ilmu,2006.

[3] Munir, Rinaldi, Kriptografi, Penerbit Informatika, Bandung,2006