Triad Primus Cipher

Rifkiansyah Meidian Cahyaatmaja
13511084
Teknik Informatika ITB
Bandung, Indonesia
rifkiansyahmeidian@gmail.com

Michael Alexander Wangsa
13512046
Teknik Informatika ITB
Bandung, Indonesia
michaelaw320@gmail.com

***Abstract*—Algoritma Block Cipher merupakan salah satu algoritma yang digunakan luas dalam kriptografi. Algoritma ini bekerja menggunakan algoritma deterministik pada sebuah kelompok bit berukuran tetap. Algoritma Thorp Shuffle adalah salah satu algoritma yang menggunakan Block Cipher. Akan tetapi, algoritma Thorp Shuffle tidak efektif untuk mengenkripsi pesan yang panjang. Paper ini membahas mengenai sebuah improvisasi dari algoritma Thorp Shuffle untuk menambah kecepatan enkripsi dan juga keamanan menggunakan shift bit dan Unbalanced Feistel Network.**

***Keywords*—Block Cipher, Thorp Shuffle, Bit Shift, Unbalanced Feistel Network**

I. PENDAHULUAN

Block Cipher merupakan sebuah algoritma enkripsi yang sangat sering digunakan. Banyak variasi enkripsi yang menggunakan block cipher sebagai dasar dari enkripsi. Block cipher sendiri dasarnya adalah penggunaan sebuah blok kunci untuk mengenkripsi sebuah pesan dimana setiap blok kunci adalah unik. Block cipher sendiri memiliki beberapa metoda untuk memperkuat pengamanan, diantaranya adalah Iterated Cipher, dimana penggunaan algoritma diulang berkali-kali; Confusion dan Diffusion, konsep dimana pengubahan kecil dalam kata kunci atau plaintext dapat berpengaruh besar pada hasil ciphertext; Feistel Network, sebuah jaringan yang digunakan untuk mengacak plaintext ketika dienkripsi menjadi ciphertext.

Thorp Shuffle adalah sejenis block cipher yang menggunakan Unbalanced Feistel Network[1]. ia mengganti satu bit untuk setiap iterasi, maka dapat dikatakan Thorp Shuffle sangat aman jika dibandingkan dengan jenis block cipher lainnya. Akan tetapi, karena hanya satu bit yang diubah untuk setiap iterasi, maka perubahan yang terjadi sangat lambat dan Thorp Shuffle hanya tepat digunakan untuk plaintext yang berukuran kecil. Plaintext berukuran besar membutuhkan ronde yang sangat banyak untuk mengenkripsi seluruh teks. Bagaimanapun, dengan sedikit modifikasi maka kelebihan Unbalanced Feistel Network pada Thorp Shuffle dapat digunakan sementara menjaga kecepatan enkripsi.

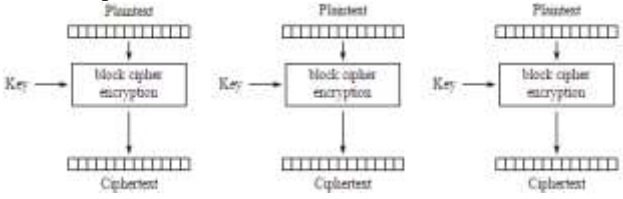
II. DASAR TEORI

A. *Block Cipher*

Block Cipher membagi plaintext menjadi beberapa blok-blok bit dengan panjang sama. Panjang kunci enkripsi dibuat sedemikian rupa sehingga sama dengan panjang blok. Enkripsi dilakukan terhadap blok bit plaintext menggunakan bit-bit kunci, dan menghasilkan blok ciphhertext yang dihasilkan panjangnya = blok plaintext.

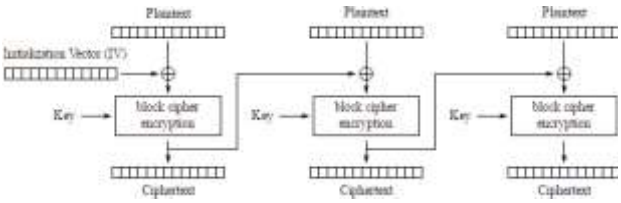
Block Cipher memiliki beberapa mode enkripsi, diantaranya yang sering digunakan adalah ECB, CBC, dan CFB[2]. Ada satu mode lagi yang terkadang digunakan yaitu OFB

ECB atau Electronic Codebook adalah mode enkripsi dimana pesan dibagi kedalam blok-blok dan setiap blok dienkripsi secara terpisah. Kekurangannya adalah blok yang serupa akan terenkripsi menjadi cipher yang serupa juga, dan maka dari itu tidak menyembunyikan pola data secara cukup baik.



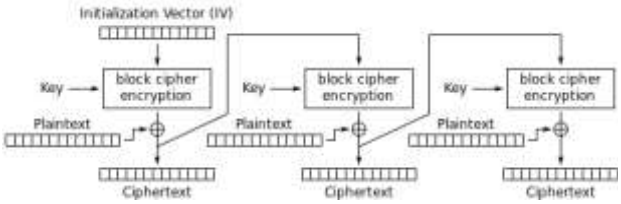
Gambar 1. Mode Enkripsi ECB,
(en.wikipedia.org/wiki/Cipher_Block_mode_of_operation)

CBC atau Cipher Block Chaining adalah mode dimana setiap blok di-XOR dengan blok cipher sebelumnya sebelum dienkripsi. Dengan cara ini maka setiap blok cipher tergantung pada semua blok plaintext yang diproses hingga titik tersebut.



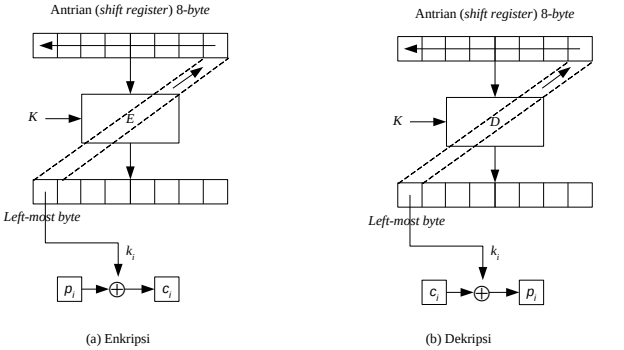
Gambar 2. Mode Enkripsi CBC, (en.wikipedia.org/wiki/Cipher_Block_mode_of_operation)

CFB atau Cipher Feedback mirip dengan CBC. CFB menggunakan hasil ciphertext dari blok sebelumnya sebagai *stream cipher* untuk blok yang tengah dienkripsi.



Gambar 3. Mode Enkripsi CFB, (en.wikipedia.org/wiki/Cipher_Block_mode_of_operation)

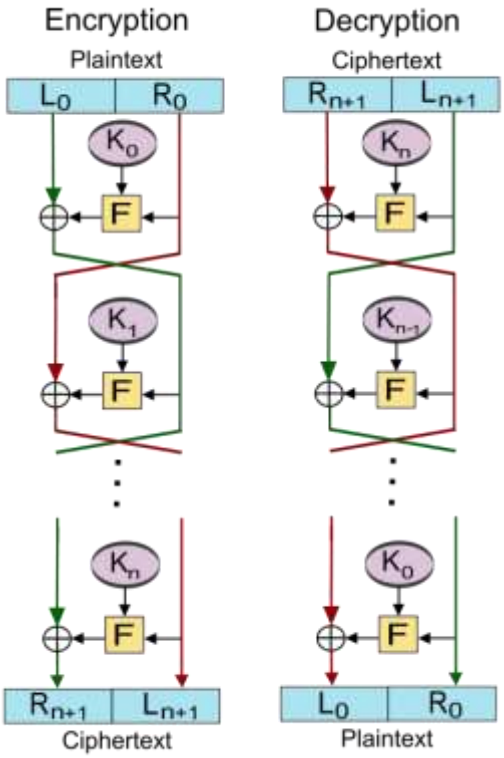
OFB atau Output-Feedback mirip dengan mode CFB, namun n-bit hasil enkripsi terhadap antrian disalin menjadi elemen posisi paling kanan di antrian.[4]



Gambar 4, Mode Enkripsi OFB (Slide Algoritma Kriptografi Modern)

B. Feistel Network

Feistel Network merupakan sebuah struktur simetrik yang digunakan dalam pembuatan block cipher. Struktur ini dapat digunakan dalam satu arah untuk melakukan enkripsi, atau dalam arah sebaliknya untuk melakukan dekripsi. Hal ini memudahkan enkripsi dan dekripsi jika seseorang memiliki kunci yang tepat.

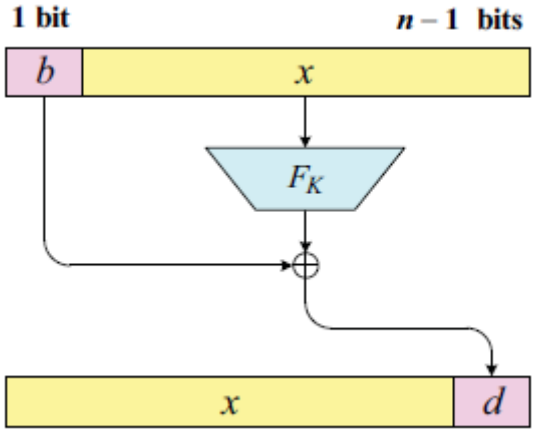


Gambar 4. Contoh Feistel Network(en.wikipedia.org)

Feistel Network umumnya membagi plaintext kedalam dua buah bagian dimana untuk kedua bagian itu diterapkan sebuah algoritma yang berbeda untuk membentuk ciphertext. Sebuah upakunci(subkey) dimasukkan di setiap bagian Feistel Network dimana bagian ini diulang beberapa kali sehingga plaintext terenkripsi beberapa kali.

Feistel Network memiliki sebuah varian yang disebut Unbalanced Feistel Network dimana penggunaan Feistel Network tidak simetris pada kedua sisi Feistel Network. Sisi kanan dan sisi kiri memiliki panjang yang berbeda.

Thorp Shuffle adalah jenis Unbalanced Feistel Network dimana sisi kiri hanya memiliki satu bit sementara sisi kanan teridri atas sisa dari teks.



Gambar 5. Thorp Shuffle Cipher.

Thorp Shuffle dinilai sangat aman karena setiap bit dienkripsi secara khusus, sehingga menyulitkan dekripsi. Di sisi lain, Thorp Shuffle tidak cocok untuk enkripsi teks yang sangat panjang karena akan membutuhkan ronde yang amat banyak untuk mengenkripsi seluruh pesan.

C. *Confusion and Diffusion*

Confusion dan *Diffusion* adalah dua sifat dari operasi enkripsi yang aman. Definisi confusion adalah membuat hubungan antara kunci dan ciphertext serumit mungkin. Diffusion mengacu kepada sifat dimana pengulangan dalam statistik plaintext menjadi 'kabur' dalam statistik ciphertext.[3]

Salah satu tujuan confusion adalah membuat kunci sangat sulit ditemukan bahkan setelah ditemukan pasangan plaintext-ciphertext yang diciptakan dengan kunci yang sama. Salah satu cara paling sederhana untuk mencapai confusion dan diffusion adalah menggunakan jaringan substitusi-permutasi dan pengulangan cipher.

D. S-Box

S-Box atau Substitution Box adalah sebuah komponen dasar dari algoritma kunci simetri yang melakukan substitusi. Secara umum, sebuah S-box mengambil beberapa bit masukan dan mengubahnya kedalam beberapa bit keluaran dimana masukan dan keluaran mungkin berbeda. Hasil bit keluaran tersebut akan mengaburkan hubungan antara kunci dan ciphertext dan memberikan sifat *confusion* pada cipher.

E. Struktur Thorp Shuffle

Secara aljabar, struktur Thorp Shuffle dapat dijelaskan sebagai berikut:

Mengacu pada gambar 5, untuk setiap ronde r=1,2…R, bit pertama pada posisi x dan x+N/2, dimana $x \in \{0, \ldots, N/2 - 1\}$, dipindahkan kepada posisi 2x dan 2x+1 atau sebaliknya 2x+1 dan 2x dimana hal tersebut ditentukan sebuah lemparan koin. $c \in \{0, 1\}$. Th[N,R] menandai Thorp Shuffle dengan ruang pesan M = {0,…,N-1}

Karena diperlukan *n* ronde dari sebuah *unbalanced feistel* maksimal, hingga setiap bit diubah, maka diperlukan *n* ronde dari sebuah *unbalanced feistel* maksimal agar cipher dapat dibilang memenuhi standar.

Asumsikan $N = 2^n$, r>=1, dan Cipher yang digunakan Th[N,R] yaitu Thorp Shuffle dengan R=2rn ronde, maka sebuah serangan menggunakan plaintext terpilih yang nonadaptif menggunakan query sejumlah *q* memiliki kemungkinan membedakan cipher paling banyak $(q/(r + 1)) \cdot (4nq/N)_r$ dari permutasi random yang terdiri atas *n* bit.

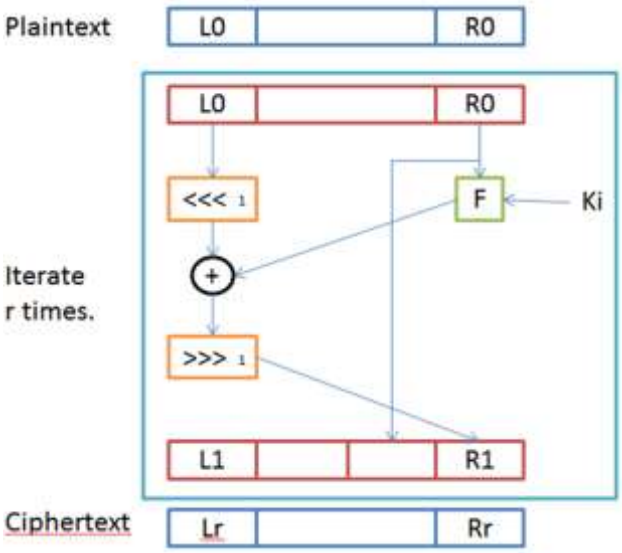
Thorp Shuffle juga memiliki sifat rantai Markov. Dengan Ω sebuah set tak kosong dan μ, ν sebagai distribusi probabilitas dari Ω, sebuah *coupling* dari μ dan ν adalah pasangan variabel acak (X,Y) yang didefinisikan dalam ruang probabilitas yang sama, sehingga distribusi marginal X dan Y adalah μ dan ν. Didapatkan:

$$\|\mu - \nu\| = \max_{S \subset \Omega} \mu(S) - \nu(S) = \min_{X \sim \mu,\, Y \sim \nu} \mathbf{P}(X \neq Y)$$

sebagai jumlah variasi jarak antara μ dan ν dimana $Z \sim \tau$ berarti Z memiliki distribusi τ.

III. TRIAD PRIMUS CIPHER

Usulan yang diajukan dalam paper ini adalah improvisasi dari Thorp Shuffle, namun menggunakan modified Feistel Cipher. Dibandingkan dengan Thorp Shuffle dimana sisi kiri terdiri atas satu bit dan sisi kanan sisa bit dari blok, Triad Primus Cipher mengambil dua bit dari sisi kiri dan dua bit dari sisi kanan untuk untuk dimasukkan kedalam sebuah Feistel Network.



Gambar 6. Triad Primus Cipher.

1. L0 dan R0 masing-masing berukuran 2 bit dan akan digunakan dalam enkripsi. Jika teks berukuran kurang dari 4 bit, maka teks akan dibagi dua seperti Feistel Network biasa.
2. Feistel Network idealnya dijalankan sebanyak block size/2 setiap ronde.
3. L0 = Blok Kiri
   R0 = Blok Kanan
   F = Fungsi enkripsi
   Ki = Upakunci pada ronde tersebut.
4. Shift yang digunakan adalah Circular Shift, dalam Triad Primus berfungsi sebagai bit switch operator.

Secara sederhana, Triad Primus hanya mengambil 2 bit paling kiri dan paling kanan, kemudian mengaplikasikan pengubahan yang berbeda kepada keduanya: Kepada dua bit kiri, dilakukan shift kiri satu kali; kepada dua bit kanan, dilakukan aplikasi fungsi dengan kunci. Setelah didapatkan hasil dari keduanya, dilakukan XOR dari keduanya dimana hasil dari XOR kemudian dilakukan shift kiri satu kali untuk menambah sifat confusion, kemudian hasil dari shift tersebut dipindahkan menjadi dua bit paling belakang, dan sisa dari bit digeser kedepan.

Satu ronde Triad Primus dijalankan sebanyak block size/2, yang dalam paper ini digunakan block size sebesar 64-bit dimana dihasilkan 32 kali aplikasi Feistel Network agar seluruh plaintext terenkripsi.

IV. Implementasi dan Kinerja

A. Implementasi

Implementasi dilakukan dengan menggunakan C++. Program dapat melakukan enkripsi block cipher dalam mode ECB, CBC, dan CFB 8-bit.

Enkripsi dilakukan pertama dengan membaca file, yang kemudian diubah menjadi blok-blok berukuran 64-bit. Setelah itu dilakukan pemilihan mode ECB, CBC, atau CFB 8-bit. Setelah mode dipilih, maka dilakukan operasi Feistel Triad Primus menggunakan cipher yang telah dipilih. Default ronde yang dapat digunakan bisa dipilih, dimana defaultnya adalah 8 ronde aplikasi penuh Feistel Triad Primus untuk menjamin *confusion* dan *diffusion* dengan *iterated cipher*.

Setelah itu, ciphertext hasil feistel akan disubstitusi menggunakan S-Box berdasarkan kunci untuk memperkuat efek diffusion, dimana setelahnya akan dilakukan juga pengacakan menggunakan sebuah *seed* berdasarkan kunci untuk lebih jauh memperkuat efek confusion. Hasil enkripsi inilah yang kemudian dituliskan dalam file.

Dekripsi dilakukan pertama dengan membaca file ciphertext yang diubah kembali menjadi blok-blok, yang kemudian dikembalikan ke posisi semula dari pengacakan menggunakan *seed* berdasarkan kunci yang sama, lalu disubstitusi balik dengan S-Box berdasarkan kunci yang sama dengan ketika dilakukan enkripsi.

Setelah disubstitusi balik, maka dilakukan pemilihan mode operasi ECB, CBC atau CFB 8-bit untuk kemudian diaplikasikan Feistel Network Triad Primus secara kebalikan untuk keperluan dekripsi. Hasil dari feistel network ini lalu akan ditulis di akhir.

Kunci digunakan sebagai seed untuk Pseudo Random Number Generator yang digunakan dalam pengacakan blok, substitusi blok, serta subkey untuk *round function* feistel Triad Primus. Substitusi dan transposisi level bit dilakukan dengan feistel Triad Primus, substitusi level byte menggunakan S-Box, sementara pada level blok dengan pengacakan, yang telah dijelaskan sebelumnya.

Untuk kunci yang digunakan jika panjangnya kurang maka akan dilakukan padding berupa pengulangan kunci. Jika panjang kunci lebih maka akan dilakukan pemotongan secukupnya sehingga mengikuti panjang blok yaitu 64-bit. Initialization Vector dibangkitkan secara acak menggunakan seed dari fungsi time(NULL).

Cipher dapat diaplikasikan ke berbagai jenis binary file, tidak terbatas hanya pada teks saja.

B. Kinerja

Dilakukan pengujian menggunakan mode CBC terhadap sebuah *file* video berukuran 440 MB dengan format .mkv menggunakan *default round* sebanyak 8 *round*. Waktu yang dibutuhkan untuk melakukan enkripsi yaitu 5 menit, sementara waktu yang dibutuhkan untuk melakukan dekripsi yaitu 6 menit 32 detik.

Pengujian menggunakan mode ECB memberikan hasil serupa yaitu enkripsi selama 4 menit 53 detik sementara dekripsi selama 6 menit 20 detik. Pengujian menggunakan mode CFB hanya berbeda sedikit dengan mode CBC yaitu 5 menit 2 detik dan dekripsi sebesar 6 menit 34 detik.

V. Kesimpulan

Algoritma Cipher Triad Primus meningkatkan waktu pemrosesan terhadap berkas berukuran besar jika dibandingkan dengan algoritma Thorp Shuffle biasa. Dengan keandalan keamanan Thorp Shuffle dan kecepatan yang lebih tinggi, Triad Primus menjadi sebuah pilihan yang dapat dipertimbangkan sebagai sebuah algoritma kriptografi.

VI. Lampiran

Triad Primus Cipher dapat diakses di https://github.com/michaelaw320/TriadPrimus-Cipher

Daftar Pustaka

[1] Morris, Ben et. al. *How to Encipher Messages on a Small Domain*
Deterministic Encryption and the Thorp Shuffle. 2009.

[2]en.wikipedia.org/wiki/Block_cipher_mode_of_operation, dikunjungi terakhir 23/03/2016.

[3]http://cryptography.wikia.com/wiki/Confusion_and_diffusion, dikunjungi terakhir 23/03/2016

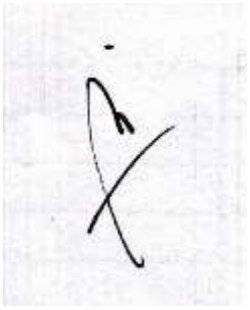
[4]Slide Algoritma Kriptografi Modern oleh Rinaldi M., tahun 2016.

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, 16 Maret 2016

ttd



Rifkiansyah Meidian C.

Michael Alexander W.