ANALISIS DAN IMPLEMENTASI KEAMANAN METODE ENKRIPSI ALGORITMA SERPENT

Asep Supriatna [1], Manahan P. Siallagan [2], Budhi Irawan [3]
Teknik Informatika
Universitas Komputer Indonesia
Jalan Dipati Ukur 112-114 Bandung 40134
Phone: +62226027706 / +628156162601
Email: Scoutland_2004@yahoo.com

ABSTRACT

Cryptography is a saint which use a linear mathematic to processed data encryption or decryption. This technique to use for converting or change data to be a code specially, with for information save or to transmission with network not to safe (like internet), can't read from whoever except the people which can be read [1].

This research analyzed about data security at the information system environment. Where in this journal will be elaborated about a security model use modern encryption technique which are using Serpent algorithm, that is become famous which are the AES candidate block cipher.

The main algorithm is part of three group they are is Initial Permutation, thirty two rounds consisting of a round Function that performs key masking, S-Box Substitution, and (in all but the last round) data mixing via a linear transformation and Final Permutation. If used on communication system then between sender and receiver must take some secret key, to used encrypt and decrypt data to send/received [2] .

ABSTRAK

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi data. Teknik ini digunakan untuk mengkonversi atau mengubah data kedalam bentuk kode-kode tertentu, dengan tujuan informasi yang disimpan maupun ditransmisikan melalui jaringan yang aman (misalnya internet), tidak dapat terbaca oleh siapapun kecuali oleh orang-orang yang berhak [1] .

Penelitian ini menganalisis tentang keamanan data pada lingkungan sistem informasi. Dimana pada jurnal ini akan diuraikan tentang sebuah model security menggunakan teknik enkripsi modern yaitu dengan menggunakan algoritma Serpent, yang terkenal menjadi salah satu kandidat blok cipher AES.

Algoritma utama serpent dibagi menjadi tiga bagian yaitu Inisial Permutasi, Operasi 32 Putaran kecuali pada putaran terakhir dan pencampuran data pada transformasi linear, dan Final permutasi. Jika digunakan dalam sistem komunikasi maka antara pengirim dan penerima harus memiliki kunci rahasia yang sama, yang dapat digunakan untuk mengenkrip dan mendekrip data yang dikirim/diterima [2].

PENDAHULUAN

Saat ini perkembangan sangat cepat dan pesat dibidang teknologi informasi atau lebih dikenal dengan sebutan IT memberikan pengaruh yang lebih besar dan banyak pada berbagai aspek kehidupan manusia, didukung pula perubahan pada perangkat keras (*hardware*) dan perangkat lunak (*Software*) yang terus menerus, untuk menunjang kemudahan bagi banyak orang dalam memenuhi kebutuhan informasi [3].

Keamanan sistem informasi dari data yang kita buat sangat berperan penting, untuk menunjang keaslian dari data tersebut agar tidak mudah dirubah oleh orang yang tidak bertanggungjawab [3].

Banyak sekali permasalahan seperti data asli hilang, meskipun telah menggunakan pengamanan data seperti *password* tetap saja ada yang sanggup menembusnya [3].

Dilandasi persoalan tersebut maka akan lebih baik jika semua orang menggnakan sistem pengamanan data yang agak sulit ditembus, seperti enksipsi dan dekripsi data pada kriptograpi [3].

Kriptograpi secara umum digunakan dalam bidang keamanan informasi, teknik yang digunakan adalah mengkonversikan data kedalam bentuk tertentu seperti menggunakan persamaan matematis contohnya algoritma kriptografi [3].

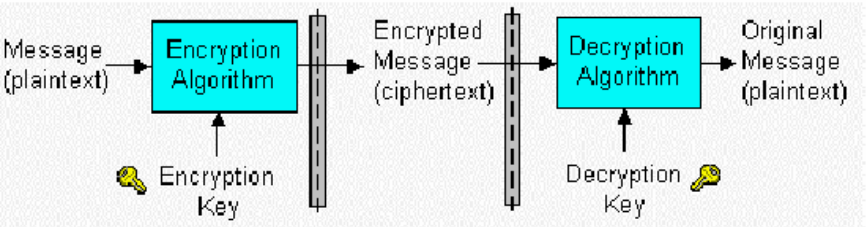
Jika data penting seperti arsip dan lain sebagainya dibuat dengan sistem keamanan yang menggunakan algoritma kriptografi yang dapat mengenkripsi maupun mendekripsi data, maka keamanan data tersebut besar kemungkinan datanya terjamin untuk periode waktu yang sangat lama[3].

Batasan Masalah

Dalam penulisan tugas akhir ini penulis akan membatasi masalah pada beberapa hal berikut ini :

1. Menganalisa kinerja dari algoritma serpent sejauh mana sistem keamanan dari data yang diterapkan dengan menggunakan algoritma tersebut.
2. Mengimplementasi metode ini dengan menggunakan software yang telah dirancang untuk memberikan gambaran tentang model keamanan menggunakan algoritma enkripsi.

Berikut ini adalah skema pemrosesan dari metode enkripsi yang diterapkan untuk model keamanan.



Gambar 1 Proses Pengenkripsian Data

Perkembangan Menuju Algoritma Serpent

Suatu pemikiran yang dilakukan untuk pendekatan baru terhadap kriptografi diawali oleh DES (*Data Encryptions Standard*), walaupun secara teroritis handal terhadap *Brute Force Attack* (mencoba satu persatu kombinasi yang mungkin), memiliki ketergantungan keamanan yang sangat tinggi terhadap kerahasiaan *key* yang digunakan. *Key* dapat dianggap sebagai password dan password terkadang dilakukan dengan tidak hati-hati oleh pemiliknya, misalnya ditulis ditempat yang dapat ditemukan oleh orang lain, atau dicuri dari sistem pengelolaa *key* untuk DES disebut sebagai *Key Distribution Center [3].*

Dalam kriptografi konvensional atau lebih sering disebut kriptosistem simetris satu buah kunci digunakan dalam dua proses, yaitu enkripsi dan dekripsi. DES merupakan nama dari sebuah pengenkrip data (DEA : *Data Encryption Algorithm*) yang dikeluarkan oleh *Federal Information Processing Standard* (FIPS) Amerika Serikat [3] .

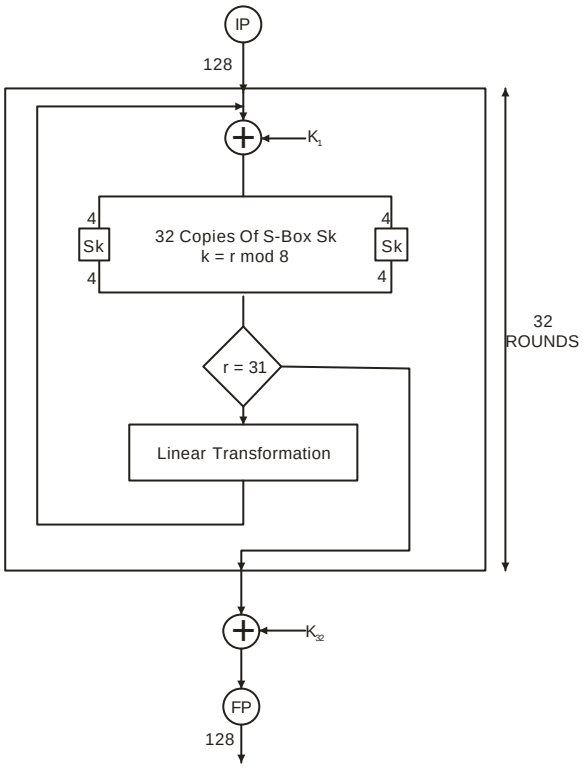
Algoritma dasarnya sendiri (dikenal dengan nama Lucifer) dikembangkan oleh IBM, NSA (sekarang lebih dikenal dengan NIST), dan NBS yang berperan penting dalam penembangan bagian akhir dari algoritmanya. DEA dan DES telah dipelajari secara eksentif sejak publikasi pertamanya. Akan tetapi setelah beberapa lama bertahan keberadaannya, NIST Amerika mensertifikasi ulang DES setiap lima tahun. DES terakhir disetifikasi ulang tahun 1993, kini NIST tidak lagi mensertifikasi DES disebabkan banyaknya kelemahan DES dan adanya pengembangan algortima baru yaitu *Advance Encryption Standard* (AES). Yang kemudian seperti diharapkan semua orang yaitu dimasa yang akan datang AES dapat mengembangkan DES dan ternyata harapan tersebut dapat terjadi muncul kembali beberapa algoritma yang diharapkan dapat menjadi standard enkripsi diantaranya ialah Algortima Serpent, yang merupakan perkembangan dari AES [3].

Proses Enkripsi Algoritma Serpent

Algoritma Serpent adalah Subtitusi Permutasi (SP) yang beroperasi didalam 32 bit masukan. Algoritma ini mengenkripsi dan mendekripsi dengan masukan 128 bit dengan sebuah kunci 128, 192 atau 256 bit panjangnya. Algoritma serpent tediri dari tiga komponen utama yaitu [2] :

1. Inisial Permutasi (IP)
2. 32 Putaran yang terdiri dari operasi pertukaran, kecuali di putaran terakhir dan pencampuran data pada transformasi linear.
3. Final Permutasi (FP)

Adapun untuk lebih jelasnya, struktur algoritma serpent digambarkan seperti berikut [2] :



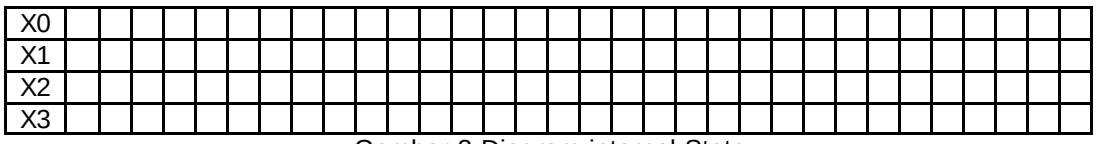
Gambar 2 Alur Algoritma Enkripsi Serpent

Dari gambar diatas maka plain teks yang dimasukan akan dilakukan proses pertukaran dengan menggunakan metode matrik transposisi yaitu pertukaran dari plain teks, sehingga setelah di lakukan inisial permutasi maka sudah tentu plain teks yang dimasukan sudah tidak terbaca lagi sebagai teks biasa, setelah di lakukan transposisi maka mulai dimasukan kunci yang akan dibawa selama ia melakukan transposisi yang kemudian di exclusive -or kan dengan Salt key lalu pada perputaran Kotak S dilakukan teknik transposisi kembali selama 31 kali dengan hasil akhir di lakukan transformasi linear, Serpent menggunakan delapan Kotak-S yaitu S_0,……S_7. Kotak-S pada serpent mengambil 4 masukan bit dan memproses 4 keluaran bit pula. Pertimbangkan aplikasi dari Kotak-S yaitu S_i ke 128 bit blok X_i. Kemudian algoritma ini memisahkan X_i kedalam 4 kotak yang terdiri dari 32 bit yaitu X_0, X_1, X_2, X_3. Untuk setiap posisi-posisi 32 bit, kemudian Serpent membangun dari bit yang berkoresponden di setiap 4 kata dengan bit dari X_3 yang merupakan bit paling signifikan, kemudian serpent menerapkan Kotak-S S_i kedalam kotak yang dikonstruksikan dan menyimpan hasil kedalam bit repektif **Y_i = (yo,y1,y2,y3)**

Transformasi linear L pada **Y_i = (y0,y1,y2,y3)** ditentukan sebagai berikut [2]

$$
\begin{aligned}
X_0, X_1, X_2, X_3 &:= \mathcal{S}_i(B_i \oplus K_i) \\
X_0 &:= X_0 <<< 13 \\
X_2 &:= X_2 <<< 3 \\
X_1 &:= X_1 \oplus X_0 \oplus X_2 \\
X_3 &:= X_3 \oplus X_2 \oplus (X_0 << 3) \\
X_1 &:= X_1 <<< 1 \\
X_3 &:= X_3 <<< 7 \\
X_0 &:= X_0 \oplus X_1 \oplus X_3 \\
X_2 &:= X_2 \oplus X_3 \oplus (X_1 << 7) \\
X_0 &:= X_0 <<< 5 \\
X_2 &:= X_2 <<< 22 \\
B_{i+1} &:= X_0, X_1, X_2, X_3
\end{aligned}
$$

Dimana <<< dinotasikan sebagai rotasi kiri dan << didetonasikan sebagai shift kiri. Pernyataan tersebut akan membawa kita selalu menuju kepada diagram seperti berikut ini :



Gambar 3 Diagram internal State

Dimana X_i pernyataan internal dibawah inspeksi dan **X_i = x0,x1,x2,x3** seperti yang digambarkan pada diagram diatas, kita akan menuju ke sebuah aktif Kotak-S, sebagai "kolom".

KESIMPULAN

Setelah melakukan penelitian dalam tugas akhir ini maka didapatkan beberapa kesimpulan, yaitu :

1. Sistem keamanan data menggunakan metode enkripsi menjadi relative lebih efektif dan aman.
2. Didalam pengenkripsian suatu data diperlukan dua kunci yang tentunya lebih menjamin kerahasiaan data.
3. Pengenkripsian dalam algoritma serpent membutuhkan 32 round, dengan hal ini maka keamanan algoritma serpent lebih terjamin dari pada algoritma yang lainnya.

DAFTAR PUSTAKA

[1] Wahana Komputer, *"Memahami Model Enkripsi & Security Data"*, Andi Yogyakarta.

[2] R.J Anderson, E. bilham, LR Knudsen, *"Serpent : "A proposal for the Advanced Encryption Standard",* submitted to NIST as AES candidate,1998. Lebih lengkapnya dapat dilihat pada http://www.cl.cam.ac.uk/~rja14/serpent.html.

[3] K Yusuf, *"Kriptografi Keamanan Internet dan Jaringan Komunikasi"*, Edisi Kedua, Informatika, Bandung, 2004.