PENERAPAN METODE BLOCK CIPHER GOVERNMENT PADA APLIKASI PEMBELAJARAN KRIPTOGRAFI

Kurnia Yahya
Program Studi Sistem Informasi
STMIK Profesional Makassar
email : kurnia_yahya@stmikprofesional.ac.id

Abstrac

Cryptography is also known in the world of education, especially the field of information technology. Some lecture places are often found learning about cryptography that only deals with theories without directly seeing what is happening in the cryptographic process, so that in this final project will be made a cryptographic algorithm learning application that can simplify in learning some process that happened in cryptografi especially the standard block cipher government method. The process that occurs for the first time in this method is the process of forming keys, encryption and decryption processes that have certain functions such as substitution box, rotate left shift, XOR operation and modulo operations are elaborated with more detailed visualization and gradual data changes.

Keywords : *Cryptography, Block Cipher, Government standard*

A. PENDAHULUAN

Kriptografi adalah suatu ilmu dan seni dalam menjaga kerahasiaan suatu pesan (kode), kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Di dalam kriptografi banyak ditemukan metode-metode kriptografi, salah satu diantaranya adalah metode GOST.

Metode GOST memiliki algoritma enkripsi dengan jumlah proses sebanyak 32 *round* dan menggunakan 64 bit *block cipher* dengan 256 bit *key*. Metode GOST juga menggunakan 8 buah *Substitution Box (S-Box)* yang permanen dan operasi *XOR* serta *Rotate Left Shift*.

Setiap metode di dalam ilmu kriptografi yang digunakan untuk mengamankan data memiliki kelebihan dan kekurangannya masing-masing, namun yang menjadi permasalahan dalam memilih metode kriptografi yang cocok adalah bagaimana mengetahui dan memahami cara kerja dari metode kriptografi yang telah dijelaskan sebelumnya, oleh karena itu diperlukan sebuah aplikasi yang dapat membantu dalam mempelajari metode kriptografi tersebut.

B. METODE PENELITIAN

a. Metode GOST

GOST merupakan singkatan dari "*Gosudarstvennyi Standard*" atau "*Government Standard*". Metode GOST merupakan suatu algoritma *block cipher* yang dikembangkan oleh seorang berkebangsaan Uni Soviet. Metode ini dikembangkan oleh pemerintah Uni Soviet pada masa perang dingin untuk menyembunyikan data atau informasi yang bersifat rahasia pada saat komunikasi. Algoritma ini merupakan suatu algoritma enkripsi sederhana yang memiliki jumlah proses sebanyak 32 *round* (putaran) dan menggunakan 64 bit *block cipher* dengan 256 bit *key*. Metode GOST juga menggunakan 8 buah *Substitution-Box* (S-Box) yang berbeda-beda dan operasi *XOR* serta *Left Circular Shift*.

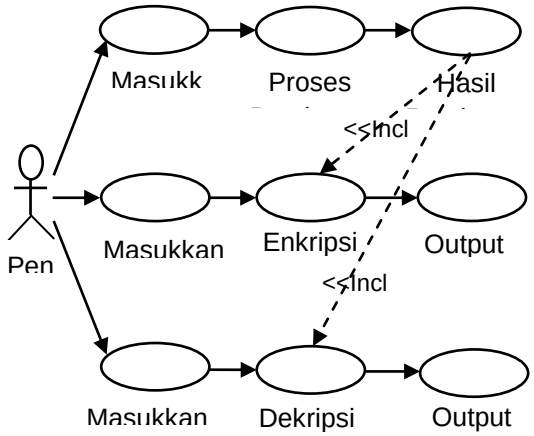
Kelemahan GOST yang di ketahui sampai saat ini adalah karena *key schedule*-nya yang sederhana sehingga pada keadaan tertentu menjadi titik lemahnya terhadap metode kriptanalisis seperti *Related-key Cryptanalysis*. Kelebihan dari metode GOST ini adalah kecepatannya yang cukup baik, walaupun tidak secepat *Blowfish* tetapi lebih cepat dari IDEA.

Komponen dari metode GOST antara lain,

1. *Key Store Unit* (KSU) menyimpan 256 *bit string* dengan menggunakan 32 *bit register* (K0, K1, …, K7).
2. Dua buah 32 *bit register* (R1, R2).
3. 32 *bit adder modulo* 2^{32} (CM1).
4. *Bitwise Adder XOR* (CM2).
5. *Substitusion block* (S) yaitu berupa 8 buah 64 *bit S-Box*.
6. *Rotasi Left shift register* (R) sebanyak 11 *bit*.

b. Use-Case Diagram

Use-case diagram dari aplikasi pembelajaran kriptografi dapat dilihat pada gambar 1.



Gambar 1. *Use-Case Diagram* Aplikasi Pembelajaran Kriptografi Metode GOST

C. HASIL PENELITIAN DAN PEMBAHASAN

Menu *Substitution Box*, menampilkan proses pengambilan nilai S-Box yang terdapat pada tabel S-Box yang nilainya permanen seperti yang terlihat pada gambar 2.

Gambar 2. Proses Subtitusi Box

Proses Pembentukan Kunci (*Key*)

Proses pembentukan kunci dapat di lihat pada penjabaran sebagai berikut :

1. *Input key* berupa 256 *bit key* dengan perincian berupa k1, k2, k3, k4, …, k256.
2. *Input key* tersebut dikelompokkan dan dimasukkan ke dalam 8 buah *key Store Unit* (KSU) dengan aturan seperti berikut :

   K0 = (k32, …, k1)

   K1 = (k64, …, k33)

   K2 = (k96, …, k65)

   K3 = (k128, …, k97)

   K4 = (k160, …, k129)

   K5 = (k192, …, k161)

   K6 = (k224, …, k193)

   K7 = (k256, …, k225)

Proses Enkripsi

Proses enkripsi pada metode GOST untuk satu putaran (iterasi) dapat di lihat dengan penjabaran sebagai berikut :

1. 64 *bit plaintext* di bagi menjadi 2 (dua) buah bagian 32 *bit*, yaitu L_i dan R_i.

   Caranya :

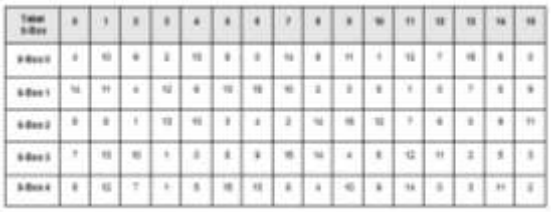
   Input A1(0), A2(0), …, A32(0), B1(0), …, B32(0)

   R_0= A32(0), A31(0), …, A1(0)

   L_0= B32(0), B31(0), …, B1(0)
2. $(R_i + K_i)$ Mod 2^{32}. Hasil dari penjumlahan modulo 2^{32} berupa 32 *bit*.
3. Hasil dari penjumlahan modulo 2^{32} di bagi menjadi 8 bagian, dimana masing-masing bagian terdiri dari 4 bit. Setiap bagian dimasukkan ke dalam tabel *S-Box* yang berbeda, 4 bit pertama menjadi *input* dari *S-Box* pertama, 4 bit kedua menjadi *input S-Box* kedua, dan seterusnya.

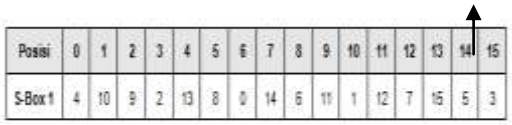
   Substitution-Box (S-Box) yang digunakan pada metode GOST adalah sebagai berikut :

Tabel.1 *Substitution-Box* pada Metode GOST



Cara melihat dari *S-Box* yaitu *input* biner di ubah menjadi bilangan desimal dan hasilnya menjadi urutan bilangan dalam *S-Box*.

Tabel 2. Cara Kerja *S-Box* pada Metode GOST



Posisi	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S-Box1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3

Tabel di atas menjelaskan bahwa jika data input ke *S-Box* adalah 5 maka di cari data pada posisi ke-5, sehingga *Output* yang dihasilkan adalah 8.

4. Hasil yang di dapat dari substitusi ke S-Box dan digabungkan kembali menjadi 32 *bit* kemudian dilakukan rotasi *left shift* sebanyak 11 bit.
5. $R_{i+1} = R_i$ (hasil dari *rotate left shift*) XOR L_i.
6. $L_{i+1} = R_i$ sebelum dilakukan proses.

Proses penjumlahan modulo 2^{32}, *S-Box*, *Rotate Left Shift* dilakukan sebanyak 32 kali (putaran) dengan penggunaan kunci pada masing-masing putaran berbeda-beda sesuai dengan aturan berikut ini :

Putaran 0 – 7 : K0, K1, K2, …, K7
Putaran 8 – 15 : K0, K1, K2, …, K7
Putaran 16 – 23 : K0, K1, K2, …, K7
Putaran 24 – 31 : K7, K6, K5, …, K0

Putaran ke-31, langkah 5 dan 6 sedikit berbeda. Langkah 5 dan 6 untuk putaran 31 adalah sebagai berikut :

R32 = R31 sebelum dilakukan proses
L32 = L31 XOR R31

Sehingga, *ciphertext* yang dihasilkan adalah

L32 : B(32), B(31), …, B(1)
R32 : A(32), A(31), …, A(1)
T = A(1), …, A(32), B(1), …, B(32)

2. Proses Dekripsi

Proses dekripsi merupakan proses kebalikan dari proses enkripsi. Penggunaan kunci pada masing-masing putaran pada proses dekripsi adalah sebagai berikut :

Putaran 0 – 7 : K0, K1, K2, …, K7
Putaran 8 – 15 : K7, K6, K5, …, K0
Putaran 16 – 23 : K7, K6, K5, …, K0
Putaran 24 – 31 : K7, K6, K5, …, K0

Algoritma yang digunakan untuk proses dekripsi sama dengan proses enkripsi dengan aturan untuk langkah 5 dan 6 pada putaran ke-31 adalah sebagai berikut :

R32 = R31 sebelum dilakukan proses.
L32 = R31 XOR L31.

Plaintext yang dihasilkan pada proses dekripsi adalah,

L32 = B(32), B(31), …, B(1)
R32 = A(32), A(31), …, A(1)
P = A(1), …, A(32), B(1), …, B(32)

E. KESIMPULAN

Penerapan Metode Block Cipher Covernment Standard pada Aplikasi Pembelajaran Kriptografi dapat memiliki proses pembentukan kunci (*key related*)

yang sederhana sehingga pada keadaan tertentu menjadi titik lemahnya untuk diserang oleh seorang kriptanalis.

Aplikasi ini memiliki fasilitas penyimpanan proses yang telah di eksekusi sebelumnya yang berbentuk sederhana yakni *text file*, sehingga dapat di buka dan dipergunakan sewaktu-waktu apabila diperlukan dan menyediakan fasilitas pengaturan kecepatan visualisasi dalam tahapan proses yang sedang berjalan.

DAFTAR PUSTAKA

[1] Herryawan, I Putu. 2010. ***Aplikasi Keamanan Data Menggunakan Metoda Kriptografi GOST***. *Edukasi*. Vol. 1 (2) : 138-149.

[2] Kromodimoeljo, Sentot. 2009. ***Teori dan Aplikasi Kriptografi***. Penerbit SPK IT Consulting, Jakarta.

[3] Kurniawan, Wiharsono. 2007. ***Kriprografi : Jaringan Komputer***. Penerbit Andi & SmitDev.Com, Yogyakarta.

[4] Marisa, Fitrya. 2005. ***Analisis Perbandingan Algoritma RC4 Stream Cipher dan GOST Block Cipher Untuk Meningkatkan Keamanan Data Pada Jaringan Client/Server***. *Skripsi*. Bandung : Program Strata I Jurusan Teknik Informatika Universitas Komputer Indonesia.