Implementasi Algoritma Modular Multiplication Based Block Cipher dalam mengamankan Data Teks

Feri Anita
STMIK Budi Darma Medan, Jl. SM.Raja No.338 Sp.Limun Medan, Sumut, Indonesia
E-Mail : ferianita@gmail.com

ABSTRACT
Securing text data is very necessary to secure a data so that it is not stolen by irresponsible parties. Cryptography is one technique that can be used to secure data, namely by encoding the original data that is understood to be incomprehensible data. Cryptography is one way that is used to secure a data. Cryptography has several algorithms, one of which is a modular mulitiplication based block cipher algorithm which is one of the classic cryptographic algorithms that uses substitution in encoding data. Modular multiplication based block ciphers use 128-bit keys and an iterative algorithm consisting of linear steps (such as XOR and key applications) and parallel applications of four non-linear substitutions that can be reversed.

Keywords: Cryptography, Implementation, Modular Multiplication based block cipher

PENDAHULUAN

Pengiriman dan penyimpanan data atau pesan melalui media elektronik sudah banyak dilakukan. Terkadang perlakuan terhadap data digital tersebut perlu dirahasiakan untuk menjamin keamanan dan keutuhan data atau pesan yang dikirimkan. Dengan demikian setiap orang yang bermaksud menyimpan sesuatu secara pribadi dan rahasia akan melakukan segala cara untuk menyimpan data atau pesan tersebut agar orang lain tidak tahu.

Modular multiplication based block cipher merupakan salah satu algoritma kriptografi klasik, yang menggunakan substitusi dalam proses enkripsinya. Substitusi ditentukan oleh sebuah operasi perkalian modulo 2^{32}-1 dengan faktor konstan. Berdasarkan cara memproses teks (*plaintext*), MMB (*Modular Multiplication based Blok cipher*) bekerja dengan menggunakan plaintext 128 *bit* dan algoritma iteratif yang terdiri dari langkah-langkah *linier* (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat subtitusi non linier yang bisa dibalik [1].

Berdasarkan uraian latar belakang di atas, maka penulis merumuskan masalah sebagai berikut :1). Bagaimana menerapkan proses enkripsi dan dekripsi menggunakan algoritma *modular multiplication based block cipher* pada data teks?, 2) Bagaimana menguji proses algoritma *modular multiplication-based blok cipher* dalam pengamanan data teks menggunakan program aplikasi *Matlab*?

Perumusan masalah di atas agar dapat lebih jelas, terdapat batasan-batasan masalah yang akan dibahas lebih khusus yang hanya difokuskan pada: 1). Panjang kunci yang digunakan adalah 128 *bit*., 2). Pengujian proses enkripsi dan dekripsi menggunakan program aplikasi Matlab.

Adapun manfaat dari penelitian ini adalah: Memahami proses enkripsi dan dekripsi dalam pengamanan data teks dan Mempersulit para *hacker* untuk mencuri atau mengetahui data rahasia.

LANDASAN TEORI

2.1 Implementasi

Implementasi adalah kegiatan akhir dari proses penerapan sistem baru dimana sistem yang baru akan dioperasikan secara menyeluruh. Implementasi bertujuan untuk melakukan proses penerapan sistem yang baru. Berdasarkan pengertian tersebut dapat disimpulkan bahwa implementasi merupakan tindakan yang dilakukan untuk melaksanakan atau merealisasikan program-program yang telah disusun demi tercapainya tujuan dari kebijakan atau program-program yang telah direncanakan [2].

2.2 Algoritma

Algoritma adalah urutan langkah yang logis untuk menyelesaikan masalah tertentu [2]. Yang ditekankan adalah urutan langkah logis, yang berarti algoritma harus mengikuti suatu urutan tertentu, tidak boleh melompat-lompat. Secara definisi, algoritma adalah alur pemikiran logis yang dapat dituangkan ke dalam bentuk tulisan. Yang ditekankan

pertama adalah alur pikiran, sehingga algoritma seseorang dapat berbeda dengan algoritma orang lain. Sedangkan penekanan kedua adalah tertulis, yang berarti dapat berupa kalimat, gambar atau tabel tertentu [3].

Algoritma adalah deretan instruksi yang jelas untuk memecahkan masalah, yaitu untuk memperoleh keluaran yang diinginkan dari suatu masukan dalam jumlah waktu yang terbatas[4]

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [4]

Adapun tujuan kriptografi adalah untuk memberi layanan keamanan (aspek-aspek keamanan) sebagai berikut:

1. *Authentication*
   Penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.
2. *Integrity*
   Keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
3. *Non-repudation*
   Merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. *Confidentiality*
   Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

2.4. Algoritma Modular Multiplication Based Blok Chiper

Kelemahan metode IDEA yang menggunakan *plaintext* 64 *bit* dan operasi perkalian modulo 216 + 1, diperbaiki oleh Joan Daemen dalam sebuah algoritma yang dinamakan MMB (*Modular Multiplication-based Block cipher*). Dengan menggunakan *plaintext* 64 *bit* (4 buah 16 *bit subblock text*), metode IDEA hanya dapat diimplementasikan pada prosesor 16 *bit*, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 *bit*. Kriptografi metode MMB menggunakan *plaintext* 128 *bit* dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik [7].

Substitusi ini ditentukan oleh sebuah operasi perkalian modulo 2^{32} – 1 dengan faktor konstan, yang memiliki tingkat sekuritas lebih tinggi bila dibandingkan dengan metode IDEA 16 yang hanya menggunakan operasi perkalian modulo 2+ 1. MMB menggunakan 32 *bit subblock text* (x0, x1, x2, x3) dan 32 *bit subblock* kunci (k0, k1, k2, k3). Hal ini membuat algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 *bit*. Sebuah fungsi non linier, f,diterapkan enam kali bersama dengan fungsi XOR.

PEMBAHASAN

3.1 Analisa

Kriptografi algoritma *Modular Multiplication Based Block Cipher* menggunakan algoritma iterative yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang ditentukan oleh sebuah *modulo* 2^{32} – 1 yaitu nilai sisa hasil bagi dengan hasil perpangkatan 2^{32} dikurang 1. Hal ini menyebabkan tingkat keamanan dari algoritma MMB menjadi lebih tinggi dan sulit untuk dipecahkan.

Sama seperti algoritma kriptografi simetris lainnya, proses penyelesaian metode MMB ini dapat dibagi menjadi 3 tahapan, yaitu:

1. Proses pembentukan kunci
2. Proses enkripsi
3. Proses dekripsi

3.1.1 Proses Pembentukan Kunci

Metode MMB ini memiliki *input* 128 *bit* kunci (*key*) yang identik dengan 32 digit heksadesimal ataupun 16 karakter yang akan dipecah menjadi 4 buah *sub* kunci (*subkey*) dengan panjang masing-masing *sub* kunci adalah sebesar 32 *bit*. Untuk lebih memahami proses pembentukan kunci pada metode MMB, diberikan sebuah contoh berikut ini:

Kunci = FERI_ANITA_ABCDE

Maka proses pembentukan kuncinya adalah sebagai berikut:

Ubah terlebih dahulu kunci ke dalam bentuk biner =

01000110010001010101001010000010101
11110100000101001110010010101
01010001000001010111110100000101010000
10010000110100010001000101

Dipecah menjadi 4 buah *sub* kunci:

K_0 = 01000110010001010101001001000001
K_1 = 01011111010000010100111001001001
K_2 = 01010100010000010101111101000001
K_3 = 01000010010000110100010001000101

3.1.2 Proses Enkripsi

Proses enkripsi dari algoritma MMB ini memiliki *input* data plainteks 128 *bit* yang identik dengan 12 digit heksadesimal atau 16 karakter. Proses enkripsi metode MMB memiliki langkah-langkah sebagai berikut:

1. Plainteks dibagi menjadi 4 buah plainteks masing-masing berukuran 32 *bit*.
2. Melakukan operasi XOR antara plainteks dengan *sub* kunci yang pertama ($K_{0)}$. Kemudian gunakan fungsi f terhadap hasil operasi XOR.
3. Melakukan operasi XOR antara plainteks dengan *sub* kunci yang kedua (K_1), kemudian gunakan fungsi f terhadap hasil operasi XOR.
4. Melakukan operasi XOR antara plainteks dengan *sub* kunci yang ketiga (K_2), kemudian gunakan fungsi f terhadap hasil operasi XOR.
5. Melakukan operasi XOR antara plainteks dengan *sub* kunci yang keempat (K_3), kemudian gunakan fungsi f terhadap hasil operasi XOR.
6. Lakukan kembali langkah 2 sampai 5 sebanyak satu kali.
7. Gabungkan keempat plainteks sehingga mendapatkan cipherteks.

Fungsi f yang digunakan adalah sebagai berikut:

1. Mengalikan hasil XOR plainteks dan kunci dengan konstanta yang sudah ditentukan kemudian di-Mod-kan dengan $2^{32} - 1$. Konstanta yang sudah ditentukan adalah sebagai berikut:
   $C = (2AAAAAAA)_{16}$
   $C_0 = (025F1CDB)_{16}$
   $C_1 = 2 * c_0$
   $C_2 = 2^3 * c_0$
   $C_3 = 2^7 * c_0$
2. Setelah mendapatkan hasil perkalian, kemudian dicari *least significant bit* (LSB) dari x_0, jika LSB dari $x_0 = 1$, maka x_0 di XOR kan dengan C jika tidak maka dilihat LSB x_3, jika LSB $x_3 = 0$ maka x_3 di XOR kan dengan C, jika tidak maka $x_i = x_{i-1}$ XOR x_i XOR x_{i+1}.

3.1.3 Proses Dekripsi

Algoritma yang digunakan pada proses dekripsi agak sedikit berbeda dengan proses enkripsi. Inti proses dekripsi dari metode MMB dapat dijabarkan seperti berikut :

1. Cipherteks dibagi menjadi 4 *subblock* yang sama besar (P_0…….P_3).
2. Melakukan operasi XOR antara cipherteks dengan kunci yang keempat (K_3), kemudian gunakan fungsi f.
3. Melakukan operasi XOR antara cipherteks dengan kunci yang ketiga (K_2), kemudian gunakan fungsi f.
4. Melakukan operasi XOR antara cipherteks dengan kunci yang kedua (K_1), kemudian gunakan fungsi f.
5. Melakukan operasi XOR antara cipherteks dengan kunci yang pertama (K_1), kemudian gunakan fungsi f.
6. Ulangi langkah 2 sampai 5 sebanyak satu kali.
7. Gabungkan 4 *subblock* sehingga didapatkan plainteks.

Fungsi f yang digunakan dalam dekripsi berbeda dengan yang digunakan dalam dekripsi, yaitu sebagai berikut:

1. Melakukan operasi XOR dengan ketentuan sebagai berikut:
   $X_i = X_{i-1}$ XOR X_i XOR X_{i+1}.

Setelah mendapatkan hasil operasi XOR, kemudian dicari *least significant bit* (LSB) dari x_0, jika LSB dari $x_0 = 1$, maka x_0 di XOR kan dengan C jika tidak maka dilihat LSB x_3, jika LSB $x_3 = 0$ maka x_3 di XOR kan dengan C, jika tidak maka $X_i = C_i * X_i$.

Setelah menganalisa bagaimana proses enkripsi dan dekripsi dengan menggunakan algoritma *Modular Multiplication Based Cipher Block*, maka pembahasannya dapat dilihat dalam contoh berikut ini:

Plaintext = AYO_KITA_NGAMPUS
Kunci = FERI_ANITA_ABCDE

1. Pembentukan kunci
   Ubah kunci ke dalam bentuk biner:
   01000110010001010101001001001001
   01011111010000010100111001001001
   01010100010000010101111101000001
   01000010010000110100010001000100
   0101
   Bagi kunci menjadi 4 buah *subkey*:
   K_0 = 01000110010001010101001001001001
   K_1 = 01011111010000010100111001001001
   K_2 = 01010100010000010101111101000001
   K_3 = 01000010010000110100010001000101
2. Proses enkripsi
   Ubah plainteks ke dalam bentuk biner

Bagi menjadi 4 *subblock*:

P_0 = 01000001010010010100111101011111

P_1 = 01001011010010010100010001000001

P_2 = 01001111010011100100011101000001

P_3 = 01001101010000000101010101010011

3. Meng-xor-kan plainteks dengan K_0

$X_0 = P_0 \oplus K_0$ =

01000001010010010100111101011111

01000110010001010101001001001001 $\oplus$

00000111000011000001110100011110

$X_1 = P_1 \oplus K_0$ =

01001011010010010100010001000001

01000110010001010101001001001001 $\oplus$

00001101000011000001011000000000

$X_2 = P_2 \oplus K_0$ =

01001111010011100100011101000001

01000110010001010101001001001001 $\oplus$

00001001000010110001010100000000

$X_3 = P_3 \oplus K_0$ =

01001101010000000101010101010011

01000110010001010101001001001001 $\oplus$

00001011000001010000011100010010

Gabungkan X_0, X_1, X_2, X_3 dan konversi ke dalam bentuk karakter dan menghasilkan cipherteks.

Hasil:

01001011010100011011010011001100011101111111100010111010000101001001001110111111111011100110110000101001010100110101100000111100100

Dalam bentuk karakter:

KQ´ÌwøºS□ÜØR¦°ô

ALGORITMA DAN IMPLEMENTASI

4.1. Algoritma Pembentukan Kunci

Proses pembentukan kunci pada metode MMB sangat sederhana. Prosedur kerja dari algoritma ini dapat dijabarkan seperti berikut :

Input : K ← Kunci

Output : K_0, K_1, K_2, K_3 ← Kunci setelah diekspansi

Proses : K/4

K_0 = K [0]
K_1 = K [1]
K_2 = K [2]
K_3 = K [3]

4.2. Algoritma Enkripsi Modular Multiplication Based Block Cipher

Prosedur kerja dari proses enkripsi ini dapat dijabarkan menjadi dua bagian besar yaitu :

Input : K ← Kunci
P ← Plainteks

Output : C ← Cipherteks

Proses :

Mulai
P/4 = P_0, P_1, P_2, P_3
For j = 1 to 2
For i = 0 to 3
$P_i = P_i$ XOR K_i
$F(P_0, P_1, P_2, P_3)$
Next i
For i = 0 to 3
$P_i = P_i$ XOR K_{i+1}
Next i
For i = 0 to 3
$P_i = P_i$ XOR $F(P_0, P_1, P_2, P_3)$ XOR K_{i+2}
Next i
Next j
Selesai

4.3. Algoritma Enkripsi Modular Multiplication Based Block Cipher

Prosedur kerja dari proses dekripsi ini dapat dijabarkan menjadi dua bagian besar yaitu :

Input : K ← Kunci
C ← Cipherteks

Output : P ← Plainteks

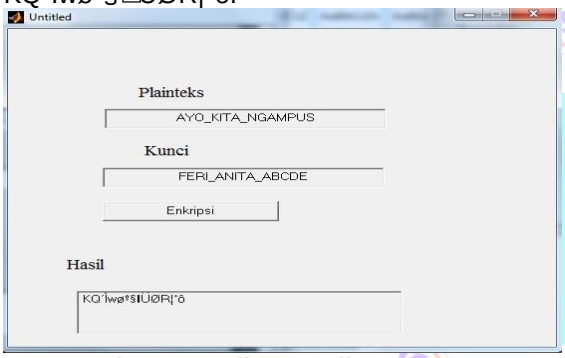
Proses :

Mulai
C/4 = C_0, C_1, C_2, C_3
For j = 1 to 2
For i = 0 to 3
$X_i = C_i$ XOR K_{i+2}
$F(C_0, C_1, C_2, C_3)$
Next i
For i = 0 to 3

$C_i = C_i$ XOR K_{i+1}
$F(C_0, C_1, C_2, C_3)$
Next i
For i = 0 to 3
$C_i = C_i$ XOR K_i
$F(C_0, C_1, C_2, C_3)$
Next i
Next j
Selesai

4.2. Implementasi

Pengujian terhadap algoritma *modular multiplication based block cipher* dengan menggunakan aplikasi program Matlab 6.1 dilakukan untuk mengetahui apakah algoritma dapat mengenkripsi atau mengamankan suatu data teks [6][8]. Berikut adalah hasil dari pengujian yang dilakukan. Pada gambar berikut dilakukan pengujian dengan masukan plainteks AYO_KITA_NGAMPUS dan kunci FERI_ANITA_ABCDE, kemudian didapatkan hasil enkripsi atau cipherteks KQ´ÌwøºS□ÜØR¦°ô.



Gambar 1 Hasil pengujian pertama

KESIMPULAN

Berdasarkan pembahasan sebelumnya, maka dapat diambil kesimpulan-kesimpulan. Adapun kesimpulan-kesimpulan tersebut adalah sebagai berikut:

1. Algoritma *modular multiplication based block cipher* mengenkripsi data menggunakan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi parallel dari empat substitusi non linier.
1. Pengujian algoritma *modular multiplication based block cipher* dilakukan dengan menggunakan program aplikasi Matlab 6.1 dengan memasukkan data teks serta kunci kemudian akan diproses dengan sebuah tombol enkripsi yang telah disisipi algoritma tersebut.

DAFTAR PUSTAKA

[1]. Mukhlisulfatih Latief. (2010). Studi perbandingan Enkripsi Menggunakan Algoritma IDEA dan MMB
[2]. Suarga. (2006). Algoritma dan Pemrograman. Yogyakarta: Penerbit Andi.
[3]. Ariyus, Dony. (2008). Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Yogyakarta: Penerbit Andi.
[4]. Munir, Rinaldi. (2006). Kriptografi. Bandung: Informatika Bandung.
[5]. Munir, Rinaldi. (2011). Algoritma dan Pemrograman. Bandung: Informatika Bandung.
[6]. Nugroho, Adi. (2010). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP. Yogyakarta: Penerbit Andi.
[7]. Rachmat C, Antonius. (2010). Algoritma dan Pemrograman dengan Bahasa C-Konsep, Teori & Implementasi. Yogyakarta: Penerbit Andi.
[8]. Sadikin, Rifki. (2010). Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Yogyakarta: Penerbit Andi.