JURNAL DASI ISSN: 1411-3201
Vol. 12 No. 1 MARET 2011

OPERASI *MIXCOLUMNS* PADA ALGORITMA RIJNDAEL

Krisnawati
STMIK AMIKOM Yogyakarta
krisna@amikom.ac.id

ABSTRAKSI

Salah satu langkah yang harus dilakukan dalam algoritma kriptografi *Rijndael* adalah transformasi *mixcolumns*. Transformasi *mixcolumns* akan mengalikan setiap kolom dari *array state* dengan suatu polinom $a(x)$ mod $(x^8+x^4+x^3+x+1)$. Proses perkaliannya mengikuti aturan seperti pada saat mengalikan matrik. Setiap kolom diperlakukan sebagai polinomial 4-suku pada *Galois Field*(2^8).

Perkalian array state dengan x dapat juga direpresentasikan dengan menggunakan *left shift* dan operasi logika XOR.

Kata Kunci *: mixcolums , Galois Field(2^8), left shift dan XOR*

PENDAHULUAN

Teknologi informasi yang berkembang sedemikian pesat menyebabkan perkembangan yang sangat signifikan pula dibidang komunikasi data. Pertukaran file dalam jaringan computer merupakan aktifitas yang sangat banyak terjadi. Sistem keamanan data menjadi hal yang mutlak agar data yang terkirim tidak diketahui pihak lain. Salah satu cara untuk mengamankan data adalah dengan memanfaatkan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*message*).

Ada dua macam kriptografi yakni:

a. Kriptografi klasik, yang bekerja berdasarkan prinsip substitusi dan transposisi, dalam mode karakter..
b. Kriptografi modern, yang menggabungkan prinsip dari kriptografi klasik dan operator logika (terutama XOR), dalam mode bit.

Salah satu algoritma kriptografi modern adalah Algoritna Rijndael. Algoritma ini juga merupakan salah satu algoritma kriptografi simetri berbasis *chipper* blok. *National Institute of Standards and Technology* (*NIST*) memilih algoritma Rijndael ini sebagai standar baru yang diberi nama *Advanced Encryption Standart (AES)* untuk menggantikan standar sebelumnya *Data Encryption Standart (DES)*.

Ada tiga macam varian AES berdasarkan panjang kunci yang digunakan, antara lain:

1. AES-128, panjang kunci 128 bit (4 word), dilakukan sebanyak 10 putaran.
2. AES-192, panjang kunci 192 bit (6 word), dilakukan sebanyak 12 putaran.
3. AES-256, panjang kunci 256 bit (8 word), dilakukan sebanyak 14 putaran.

Tahapan-tahapan yang harus dilakukan pada Algoritma Rijndael adalah sebagai berikut:

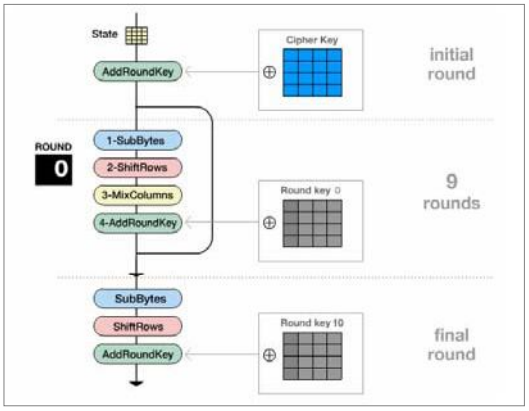
1. *AddRoundKey*: melakukan *XOR* antara *state* awal (plainteks) dengan *cipher key*. Tahap ini disebut juga *initial round*.
2. Putaran sebanyak Jumlah Putaran – 1 kali (menyesuaikan dengan varian AES yang akan dipakai). Proses yang dilakukan pada setiap putaran adalah:
   a. *SubBytes*: substitusi *byte* dengan menggunakan table substitusi (*S-box*).
   b. *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
   c. *MixColumns*: mengacak data di masing-masing kolom *array state*.
   d. *AddRoundKey*: melakukan XOR antara *state* sekarang *round key*. *Round Key* dibangkitkan dengan metode tersendiri yang salahn satunya memanfaatkan table substitusi (*S-box*).
3. *Final round*: proses untuk putaran terakhir (sama seperti langkah 2, tetapi tanpa menggunakan MixColumns) :
   a. *SubBytes*
   b. *ShiftRows*
   c. *AddRoundKey*

Contoh: Jika memilih varian AES-128 maka proses dilakukan sebanyak 10 putaran dengan rincian:

1. Proses awal (tahap 1)
2. Proses diulang sebanyak 9 putaran (proses 2 sebanyak 9 kali)
3. Proses akhir (tahap 2)

 ISSN: 1411-3201

Tahapan tersebut dapat dijelaskan dengan alur sebagai berikut:



Gambar 1: Alur proses Algoritma Rijndael (AES-128), (http://www.cs.bc.edu/~straubin/cs3805/blockciphers/rijndael_ingles2004.swf)

Dari beberapa proses yang ada pada algoritma diatas, ada satu proses yang perlu mendapatkan perhatian, dikarenakan memiliki langkah yang lebih kompleks jika dibandingkan dengan proses-proses lainnya. Proses tersebut adalah operasi *MixColumns*. Operasi ini bertujuan untuk mengacak data di masing-masing kolom array state yang diperoleh dari proses sebelumnya (proses *ShiftRows*).

PEMBAHASAN

Transformasi Mixcolumn

Transformasi *MixColumns()* dilakukan dengan mengalikan setiap kolom dari *array state* dengan polinom $a(x)$ mod $(x^8+x^4+x^3+x+1)$. Setiap kolom diperlakukan sebagai polinom 4-suku pada GF(2^8).

$a(x)$ yang ditetapkan adalah:

$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$

Transformasi ini dinyatakan sebagai perkalian matriks:

$s'(x) = a(x) \otimes s(x)$

$$\begin{bmatrix} s'_{0,1} \\ s'_{1,1} \\ s'_{2,1} \\ s'_{3,1} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,1} \\ s_{1,1} \\ s_{2,1} \\ s_{3,1} \end{bmatrix}$$

$s'_{0,1} = (\{02\} \bullet s_{0,1}) \oplus (\{03\} \bullet s_{1,1}) \oplus s_{2,1} \oplus s_{3,1}$
$s'_{1,1} = s_{0,1} \oplus (\{02\} \bullet s_{1,1}) \oplus (\{03\} \bullet s_{2,1}) \oplus s_{3,1}$
$s'_{2,1} = s_{0,1} \oplus s_{1,1} \oplus (\{02\} \bullet s_{2,1}) \oplus (\{03\} \bullet s_{3,1})$
$s'_{3,1} = (\{03\} \bullet s_{0,1}) \oplus s_{1,1} \oplus s_{2,1} \oplus (\{02\} \bullet s_{3,1})$

Proses diatas dapat diekuivalenkan juga dengan menggunakan gabungan operasi *left shift* dan operator XOR.

Misalkan diperoleh hasil *ShiftRows* sebelumnya adalah :

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Misalnya matrik hasil transformasi *Mixcolumns* disebut H, maka H didapatkan sebagai berikut:

04	e0	48	26
66	cb	f8	06
81	19	d3	26
E5	9a	7a	4c

Matriks a(x)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Dikalikan dengan hasil transformasi *ShiftRows* sebelumnya

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

Didapatkan sebagai berikut:
$H_{0,1} = (\{02\} \bullet d4) \oplus (\{03\} \bullet bf) \oplus 5d \oplus 30$
$H_{1,1} = d4 \oplus (\{02\} \bullet bf) \oplus (\{03\} \bullet 5d \oplus 30$
$H_{2,1} = d4 \oplus bf \oplus (\{02\} \bullet 5d) \oplus (\{03\} \bullet 30)$
$H_{3,1} = (\{03\} \bullet d4) \oplus bf \oplus 5d \oplus (\{02\} \bullet 30)$

Semua elemen dalam notasi heksadesimal diubah menjadi biner:
02 → 10
03 → 11
d4 → 11010100
bf → 10111111
5d → 01011101
30 → 00110000

Mengalikan array dengan polinom $a(x)$ mod $(x^8+x^4+x^3+x+1)$ pada *Galois Field*(2^8).

Mencari $H_{0,1}$

$H_{0,1} = (\{02\} \bullet d4) \oplus (\{03\} \bullet bf) \oplus 5d \oplus 30$