STUDI DAN IMPLEMENTASI ALGORITMA RIJNDAEL UNTUK ENKRIPSI SMS PADA TELEPON GENGGAM YANG BERBASIS WINDOWS MOBILE 5.0

Herdyanto Soeryowardhana – NIM : 13505095

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15095@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang studi dan implementasi Algoritma Rijndael untuk mengenkripsi data. Rijndael adalah suatu cipher blok iteratif yang memiliki suatu variabel panjang blok dan variabel panjang kunci. Panjang blok dan kunci dapat secara independen dispesifikasikan sebesar 128, 192 atau 256 bit.

SMS atau *Short Message Service* merupakan suatu layanan pengiriman pesan singkat melalui telepon genggam. Walaupun merupakan bagian dari kemampuan standard *GSM* fase pertama, *SMS* masih merupakan layanan yang banyak digunakan oleh masyarakat. Bahkan, berdasarkan survei yang dilakukan oleh Nielsen Mobile di Amerika pada kuartal 2 tahun 2008, pelanggan telepon seluler di Amerika Serikat lebih banyak menggunakan *SMS* dibanding melakukan percakapan telepon [REA08]. Berbagai kemudahan yang ditawarkan oleh *SMS*. Aplikasi enkripsi dan dekripsi pesan dapat meningkatkan tingkat keamanan pada layanan yang memerlukan kerahasiaan pesan. Hal ini dapat mengurangi bocornya informasi kepada pihak-pihak yang tidak berkepentingan seperti operator telepon seluler.

Untuk mengimplementasikan algoritma tersebut, dibuat suatu perangkat lunak bernama HSW SMS Encryptor. Perangkat lunak tersebut akan mengenkripsi SMS yang akan dikirim dari telepon seluler yang berbasis Windows Mobile 5.0. Selain itu, perangkat lunak tersebut juga dapat mendekripsi SMS yang diterima.

***Kata kunci**: Rinjdael*, *Windows Mobile 5.0*, enkripsi, dekripsi.

1. Pendahuluan

SMS atau *Short Message Service* merupakan suatu layanan pengiriman pesan singkat melalui telepon genggam. Walaupun merupakan bagian dari kemampuan standard *GSM* fase pertama, *SMS* masih merupakan layanan yang banyak digunakan oleh masyarakat. Bahkan, berdasarkan survei yang dilakukan oleh Nielsen Mobile di Amerika pada kuartal 2 tahun 2008, pelanggan telepon seluler di Amerika Serikat lebih banyak menggunakan *SMS* dibanding melakukan percakapan telepon [REA08]. Berbagai kemudahan yang ditawarkan oleh *SMS* antara lain informasi sesuai permintaan, pengunduhan nada dering, sampai dengan transaksi perbankan atau *mobile banking*.

Aplikasi enkripsi dan dekripsi pesan dapat meningkatkan tingkat keamanan pada layanan yang memerlukan kerahasiaan pesan. Hal ini dapat mengurangi bocornya informasi kepada pihak-pihak yang tidak berkepentingan seperti operator telepon seluler. Untuk meningkatkan keamanan dalam aplikasi enkripsi dan dekripsi pesan *SMS*, perlu digunakan algoritma yang handal. Salah satu algoritma yang cukup baru dan handal adalah algoritma Rijndael.

Algoritma Rijndael didesain untuk mengganti algoritma *DES* yang sudah cukup lama. Algoritma ini menggunakan kunci 128-bit, 192-bit atau 256 bit. Algoritma ini dibuat oleh dua orang periset yaitu Joan Daemen dan Vincent Rijmen. Rijndael telah dipilih oleh NIST (*National Institute of Standards and Technology*)

sebagai proposal yang paling cocok dengan kriteria keamanan, efisiensi dalam implementasi, sifat yang berubah-ubah dan kesederhanaan. Terkadang istilah AES dan Rijndael digunakan tertukar-tukar, tetapi keduanya berbeda. AES secara luas diperkirakan untuk menjadi standard utama dalam mengenkripsi semua bentuk data elektronik termasuk data yang digunakan dalam aplikasi komersial seperti perbankan dan transaksi finansial, telekomunikasi, dan informasi privat. Algoritma memiliki beberapa kelebihan antara lain relatif cepat dalam perangkat lunak dan perangkat keras, mudah untuk diimplementasikan dan hanya menggunakan memori yang kecil.

Microsoft Windows Mobile 5.0 dikeluarkan oleh perusahaan Microsoft. Sistem operasi ini sudah digunakan secara luas oleh masyarakat dan menawarkan berbagai fasilitas yang sebagian ditawarkan oleh sistem operasi Microsoft Windows versi PC. Sistem operasi ini banyak digunakan pada berbagai macam merek *PDA* (*Personal Digital Assist*). Pengembangan aplikasi pada sistem operasi ini tergolong mudah karena sudah difasilitasi dengan baik oleh Microsoft sendiri.

Makalah ini akan membahas bagaimana mengimplementasikan algoritma rinjdael untuk enkripsi dan dekripsi SMS pada telepon genggam yang berbasis Windows Mobile 5.0.

2. Tipe-tipe Algoritma Kriptografi Berbasis Kunci

Terdapat dua tipe umum dari algoritma yang berbasis kunci yaitu algoritma simetrik dan asimetrik.

2.1 Algoritma Simetrik

Algoritma simetrik adalah algoritma yang kunci enkripsinya dapat dihitung dari kunci dekripsinya dan sebaliknya. Sebagian besar algoritma simetrik menggunakan kunci enkripsi dan dekripsi yang sama. Keamanan dari dari suatu algoritma simetrik bergantung pada kunci. Jika kunci sudah diketahui, maka siapa pun dapat mengenkrip dan mendekrip pesan tersebut. Jika komunikasi harus tetap rahasia, maka kunci juga harus tetap rahasia.

Algoritma simetrik dapat dibagi menjadi 2 kategori yaitu *stream chiper* dan *block cipher*. Algoritma *stream chiper* beroperasi pada suatu bit sedangkan algoritma *block chiper* beroperasi pada kumpulan bit.

2.2 Algoritma Asimetrik

Algoritma asimetrik didesain agar kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Artinya, kunci dekripsi tidak dapat dihitung dari kunci enkripsi. Kunci enkripsi dapat disebut sebagai kunci publik sedangkan kunci dekripsi dapat disebut dengan kunci privat.

3. *Chiper* Blok

Suatu *chiper* blok mengubah suatu string dari bit-bit masukan dengan panjang tetap menjadi suatu string dari bit-bit keluaran dengan panjang tetap. Fungsi enkripsi dan dekripsi dalam algoritma intinya adalah dalam setiap bit dalam blok keluaran bergantung secara join dalam setiap bit dalam blok masukan dan setiap bit dalam kunci.

Ukuran blok chiper ditentukan oleh pertimbangan kekuatan kriptografik dan ukuran tersebut harus cukup besar untuk menghindari serangan *message exhaustion* sederhana. Sebagai contoh, dengan mencoba-coba semua kemungkinan kombinasi plainteks dengan suatu kunci yang dipilih, suatu lawan dapat membuat suatu kamus yang berisi chiperteks dan plainteks yang bersesuaian. Walaupun demikian, jika ukuran blok cukup besar, maka kamus akan terlalu besar untuk dibuat atau disimpan.

Serangan lainnya juga harus dipertimbangkan sebelum menentukan ukuran blok yang dapat diterima. Sebagai contoh, keuntungan dapat diambil dari fakta bahwa beberapa blok data lebih sering muncul dari pada yang lain. Tipe dari serangan ini disebut analisis frekuensi blok dan menggunakan metode statistik. Hal tersebut mirip dengan suatu analisis yang akan dilakukan pada suatu substitusi chiper dengan melakukan perhitungan frekuensi huruf.

Dengan mengekspresikan operasi chiper dalam bentuk matematis yang murni, maka dimungkinkan untuk memecahkan variabel yang tidak diketahui secara langsung menggunakan metode secara analitik. Pendekatan ini disebut dengan serangan deterministik. Untuk menghindari serangan tersebut, setiap bit dalam blok keluaran harus menjadi suatu fungsi matematika rumit untuk setiap bit dalam blok masukan dan kunci. Syarat ini disebut dengan dependensi antar simbol yang kuat. Dari diskusi

faktor kerja, hal tersebut harus mengikuti suatu fungsi matemtika rumit yang harus menjadi salah satu komputasinya tidak mungkin untuk dipecahkan untuk kunci tersebut, walaupun diketahui hubungan antara palinteks dan chiperteks.

Sebagai bagian dari suatu struktur matematika untuk analisis lebih lanjut, beberapa istilah yang berguna dalam suatu diskusi dari chiper blok didefinisikan dibawah ini.
X: masukan (plainteks)
Y: keluaran (chiperteks)
K: Kunci
Z: vektor inisialisasi
U: vektor inisialisasi pertengahan
R: aliran bit kriptografi

Sejak data komputer adalah format biner, notasi vektor digunakan untuk mengekspresikan suatu kuantitas. Suatu blok masukan (X) dari sejumlah b bit yang didenotasikan dengan

$$X = (x_1, x_2,....,x_b)$$

Dimana x_i adalah 0 atau 1 untuk setiap i = 1,2,...,b. Notasi |*| untuk merepresentasikan elemen-elemen pada *. Jumlah elemen pada vektor X didenotasikan oleh |X|. Pada contoh diatas, panjang dari X adalah b. Dalam beberapa keadaan, sangat membantu jika kita membicarakan suatu sekuens atau vektor sekuens waktu. Berikut adalah suatu sekuens dari n blok masukan yang didenotasikan oleh

$$(X(1), X(2), ... , X(n))$$

dan menspesifikasikan sekuens waktu atau urutan relatif dari enkripsi setiap blok. Jika setiap blok masukan mengandung b bit, lalu vektor bit masukan pada waktu ke i didenotasikan oleh

$$X(i) =(x_1(i),x_2(i), ... , x_b(i))$$

dan |X(i)| = b.

Dalam mendeksripsikan suatu chiper blok, kita tidak perlu membedakan antara enkripsi blok X pada waktu ke i dan enkripsi pada blok yang sama pada waktu ke j. Singkatnya, enkripsi dari blok X pada waktu apa saja akan menghasilkan blok Y yang sama. Tentu saja, diasumsikan bahwa kunci kriptografi yang digunakan adalah sama.

Ada operasi yang biasanya digunakan yaitu XOR dengan simbol $\oplus$.

Tabel 1 Operasi XOR

A	B	A $\oplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

Dari aturan XOR didapatkan bahwa

$$A \oplus A = 0$$
$$A \oplus 0 = A$$
$$A \oplus 1 = \bar{A}$$

dimana $\bar{A}$ merupakan komplemen dari A. $\bar{A}$ didapatkan dengan membalikan bit-bit pada A sehingga 0 menjadi 1 dan 1 menjadi 0. Oleh karena itu, jika

$$A \oplus B = C$$

maka

$$A = C \oplus B$$
$$B = C \oplus A$$

Misalnya K adalah suatu kunci dalam himpunan {K1, K2, ..., Kn} dari semua kemungkinan kunci dan f_K menjadi suatu fungsi dalam himpunan $\{f_{K1}, f_{K2}, ..., f_{Kn}\}$ dari fungsi satu-ke-satu yang berkaitan dengan kunci-kunci tersebut yang mengubah suatu blok masukan (X) dari b bit ke dalam suatu blok keluaran (Y) dari b bit. Misalnya terdapat 2^b kombinasi plainteks yang mungkin dan 2^b kombinasi chiperteks yang mungkin dalam domain dan kodomain dari setiap fungsi f_K. Secara umum, hanya kondisi $|Y| \geq |X|$ yang perlu dipenuhi untuk membuat sistem yang tidak ambigu yaitu tidak terdapat pemetaan kombinasi antara dua plainteks terhadap kombinasi cipherteks yang sama.

4. Algoritma AES atau Rijndael

4.1. Gambaran Umum Algoritma

Algoritma Rijndael secara umum dapat digambarkan sebagai berikut

- Ekspansi Kunci
- Ronde awal
    a. AddRoundKey
- Ronde
    a. SubByte

b. ShiftRows
c. MixColumns
d. AddRoundKey

- Ronde Final
  a. SubBytes
  b. ShiftRows
  c. AddRoundKey

4.2. Desain

Ada 3 kriteria dalam desain algoritma Rijndael yaitu :

- Ketahanan terhadap semua serangan yang diketahui.
- Kecepatan dan kekompakan kode dalam *platform* yang luas.
- Kesederhanaan desain.

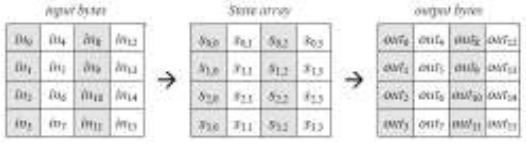
Pada sebagian besar chiper, transformasi ronde memiliki struktur feistel. Dalam struktur ini, biasanya bagian dari bit-bit pada state pertengahan secara sederhana ditranspos tanpa diubah ke posisi lainnya. Transformasi ronde pada Rijndael tidak memiliki struktur feistel.

4.1.Spesifikasi Algoritma

Rijndael adalah suatu cipher blok iteratif yang memiliki suatu variabel panjang blok dan variabel panjang kunci. Panjang blok dan kunci dapat secara independen dispesifikasikan sebesar 128, 192 atau 256 bit.

4.1.1. State, Kunci Cipher dan jumlah ronde.

Secara internal, operasi algoritma AES dilakukan pada suatu senarai dua dimensi yang berisi byte-byte yang disebut dengan *state*. Dalam state terdiri atas empat baris byte yang masing-masing mengandung Nb byte. Nb adalah suatu panjang blok yang dibagi oleh 32. Senarai state didenotasikan oleh simbol s yang masing-masing byte memiliki dua indeks yaitu nomor baris r pada range $0 \le r < 4$ dan nomor kolom c dalam range $0 \le c < Nb$. Oleh karena itu, individual byte pada state dilambangkan dengan $s_{r,c}$ atau s[r,c].



Gambar 1 Senarai State masukan dan keluaran

Kunci cipher dapat digambarkan sebagai suatu senarai persegi dengan empat baris. Jumlah kolom dari kunci cipher didenotasikan oleh Nk dan sebanding dengan panjang kunci dibagi oleh 32.

Gambar 2 Contoh kunci cipher dengan Nk = 4

Pada beberapa instans, blok-blok ini juga dapat ditentukan sebagai senarai satu dimensi dari vektor 4 byte dengan masing-masing vektor terdiri atas kolom yang bersesuaian dalam representasi senarai persegi. Senarai ini dapat memiliki panjang 4, 6, atau 8 dan indeks dengan range 0..3, 0..5, 0..7. Vektor 4 byte dapat disebut dengan istilah *word*.

Jumlah ronde yang didenotasikan oleh Nr dan bergantung kepada nilai Nb dan Nk. Diberikan pada tabel berikut.

Tabel 2 Jumlah ronde (Nr) sebagai suatu fungsi dari panjang blok dan kunci

Nr	Nb = 4	Nb = 6	Nb = 8
Nk = 4	10	12	14
Nk = 6	12	12	14
Nk = 8	14	14	14

4.1.2. Transformasi Ronde

Transformasi ronde terdiri atas empat transformasi yang berbeda yaitu:

- ByteSub
- ShiftRow
- MixColumn
- AddRoundKey

Ronde final dari cipher terdiri atas tiga transformasi yaitu:

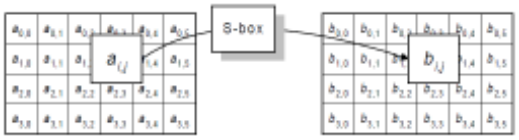
- ByteSub
- ShiftRow
- AddRoundKey

4.1.3. Transformasi ByteSub

Transformasi ByteSub merupakan suatu substitusi byte nonlinear yang beroperasi pada setiap state byte secara independen. Tabel substitusi atau S-box dapat diinvers dan dikonstruksikan oleh komposisi dari dua transformasi yaitu:

1. Pertama, ambil invers multiplikatif dalam GF(2^8).
2. Aplikasikan suatu transformasi *affine* (atas GF(2)) yang didefinisikan oleh

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$



Gambar 3 ByteSub berperan dalam individual byte dari state.

4.1.4. Transformasi ShiftRow

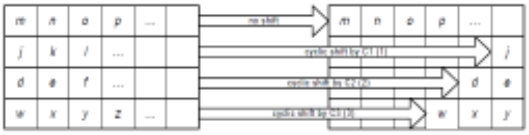
Dalam ShiftRow, baris-baris pada state secara siklik dipindahkan ke offset yang berbeda. Baris ke 0 tidak dipindahkan, baris ke 1 dipindahkan sebanyak C1 byte, baris 2 sebanyak C2 byte dan baris 3 sebanyak C3 byte.

Perpindahan offset C1, C2 dan C3 bergantung pada panjang blok Nb. Nilai yang berbeda dispesifikasikan pada tabel di bawah ini.

Tabel 3 Offset perpindahan untuk panjang blok yang berbeda.

Nb	C1	C2	C3
4	1	2	3
6	1	2	3
8	1	3	4

Gambar di bawah ini mengilustrasikan efek dari transformasi ShiftRow terhadap state.



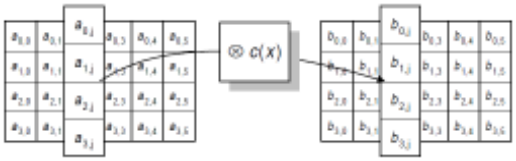
Gambar 4 ShiftRow beroperasi pada baris-baris pada state.

Invers dari ShiftRow adalah suatu perpindahan secara siklik dari 3 baris bawah ke Nb-C1, Nb-C2 dan Nb-C3 byte sehingga byte pada posisi j dalam row i berpindah ke posisi (j+Nb –Ci) modulo Nb.

4.1.5. Transformasi MixColumn

Dalam MixColumn, kolom-kolm pada state ditentukan sebagai polinomial terhadap GF(2^8) dan dikalikan modulo $x^4 + 1$ dengan polinomial tetap c(x) yang diberikan dengan

c(x) = ‘03’ x^3 +’01’ x^2 + ‘01’ x + ‘02’
Gambar di bawah ini mengilustrasikan efek dari transformasi MixColumn terhadap state.



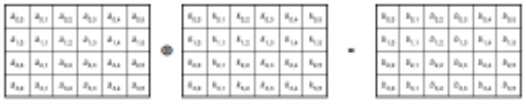
Gambar 5 MixColumn beroperasi pada kolom pada state.

Invers dari MixColumn adalah sama dengan MixColumn. Setiap kolom ditransformasikan dengan mengalikannya dengan suatu perkalian polinomial tertentu yang didefinisikan oleh
(‘03’ x^3 +’01’ x^2 + ‘01’ x + ‘02’) $\otimes$ d(x) = ‘01’.
yang diberikan oleh
d(x) = ‘0B’ x^3 + ‘0D’ x^2 + ‘09’ x + ‘0E’.

4.1.6. Penambahan Round Key

Dalam operasi ini, suatu Round Key diaplikasikan kepada state dengna suatu operasi bit EXOR. Round Key diturunkan dari kunci cipher dari jadwal kunci. Panjang Round Key ekivalen dengan panjang blok Nb.

Transformasi ini diilustrasikan pada gambar di bawah ini.



Gambar 6 Dalam penambahan kunci Round Key adalah suatu operasi bit EXOR kepada state.

4.2 Penjadwalan Kunci (Key Schedule)

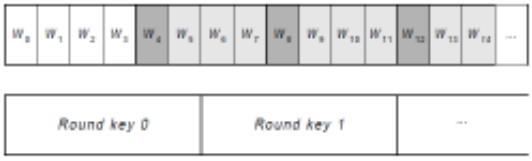
Round Key diturunkan dari kunci cipher sesuai dengan jadwal kunci. Hal ini terdiri atas dua komponen yaitu ekspansi kunci dan seleksi round key. Prinsip dasarnya adalah sebagai berikut:

- Jumlah total dari bit round key setara dengan panjang blok dikalikan dengan jumlah ronde tambah 1.
- Kunci cipher diekspansi kedalam suatu kunci yang sudah diekspansi (*expanded key*)
- Round Key diambil dari Expanded Key dengan cara Round Key pertama yang

terdiri atas Nb word pertama, kedua Nb word berikutnya dan seterusnya.

Expanded Key adalah suatu senarai linier berisi word 4 byte dan didenotasikan oleh W[Nb*(Nr+1)]. Nk word pertama berisi kunci cipher. Semua word yang lain didefinisikan secara rekursif dalam istilah word dengan indeks yang lebih kecil. Funsgi ekspansi kunci bergantung kepada nilai dari Nk.

Dalam pemilihan Round Key, Round Key ke i diberikan oelh buffer word Round Key W[Nb*i] ke W[Nb*(i+1)]. Hal ini diilustrasikan pada gambar di bawah ini.



Gambar 7 Ekspansi kunci dan pemilihan Round Key untuk Nb = 6 dan Nk = 4.

5. Pengujian

5.1 Kasus Uji Perangkat Lunak

Beberapa kasus uji yang diujikan antara lain:

- Pengujian proses pengiriman dan enkripsi SMS pada perangkat.
- Pengujian proses penerimaan dan dekripsi SMS pada perangkat serta validitas pesan yang diterima.

Gambar 8 Antarmuka halaman utama

Gambar 9Antarmuka halaman enkripsi

Gambar 10 Antarmuka halaman dekripsi

5.2 Evaluasi Hasil Pengujian

- Pesan yang dikirim dari perangkat berbasis windows mobile telah berhasil dikirim dan dienkripsi dengan baik.
- Pesan yang diterima oleh perangkat telah berhasil di terima dan didekripsi dengan baik.
- Tingkat performansi dalam proses enkripsi dan dekripsi pesan cukup cepat.

5. Kesimpulan

Kesimpulan yang dapat dimbil dari studi dan implementasi Rijndael antara lain:

- Algoritma Rijndael merupakan algoritma yang cukup handal untuk digunakan dalam enkripsi pesan – pesan yang memerlukan tingkat kerahasiaan yang tinggi.
- Algoritma Rijndael cukup cepat dalam proses enkripsi dan dekripsi.
- Algoritma Rijndael merupakan algoritma yang sederhana namun memiliki tingkat keamanan yang baik.

- Pengembangan aplikasi windows mobile cukup mudah dan difasilitasi dengan baik oleh microsoft.

DAFTAR PUSTAKA

[1] Daemen, Joan, Vincent Rijmen. (1999). AES Proposal Rijndael.

[2] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[3]Schneier, Bruce. (1996). Applied Cryptography 2nd. John Wiley & Sons.