Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular

Rangga Wisnu Adi Permana - 13504036 [1)]

1) Program Studi Teknik Informatika ITB, Bandung 40132, email: if14036@students.if.itb.ac.id

Abstract *– Pada tugas akhir ini dibangun suatu perangkat lunak yang dapat berguna untuk meningkatkan keamanan pesan yang terjadi pada komunikasi melalui SMS. SMS merupakan suatu layanan yang diberikan oleh telepon selular kepada penggunanya untuk melakukan komunikasi melalui pengiriman pesan singkat dengan biaya yang murah. SMS sangatlah populer, selain dikarenakan biayanya yang murah, pesan yang dikirimkan dapat diterima oleh penerima dengan baik dan cepat. Namun komunikasi melalui media SMS ini bukanlah komunikasi point-to-point, pesan yang dikirimkan melalui media SMS tidak langsung sampai pada tujuan, melainkan melalui jaringan SMS. Pada jaringan SMS tersebut, keamanan pesan sangatlah terancam untuk dibaca oleh orang yang tidak bertanggung jawab. Perangkat lunak yang dibangun meningkatkan keamanan pesan dengan melakukan enkripsi terhadap pesan yang dikirimkan.*

Perangkat lunak yang dibangun menggunakan algoritma RC6 untuk melakukan enkripsi SMS agar keamanan pesan dapat ditingkatkan. Algoritma RC6 adalah suatu algoritma kunci privat yang dikenal dengan kesederhanaannya. Algoritma RC6 merupakan algoritma dengan parameter yang dapat bekerja pada panjang kunci yang beragam. Untuk aspek keamanannya, algoritma RC6 mengutamakan prinsip iterated cipher.

Perangkat lunak yang dibangun menggunakan teknologi J2ME yang dapat ditanamkan pada telepon selular. Berdasarkan pengujian perangkat lunak yang dilakukan dapat dilihat bahwa perangkat lunak dapat berjalan dengan baik dan algoritma RC6 dapat diimplementasikan untuk enkripsi SMS pada telepon selular.

Kata Kunci*: SMS, RC6, iterated cipher, J2ME, enkripsi, dekripsi*

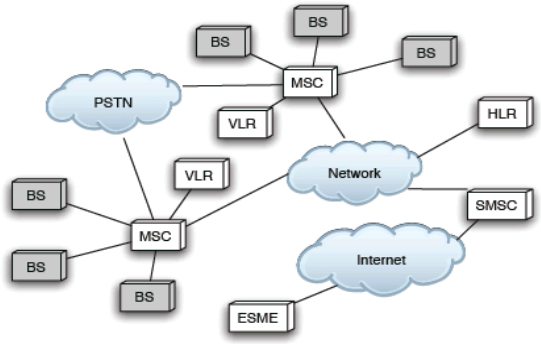
1. PENDAHULUAN

Telepon selular merupakan alat komunikasi yang sudah dipakai oleh sebagian besar orang di dunia. Telepon selular menyediakan media komunikasi yang beragam dan salah satu diantaranya adalah media SMS (*Short Message Service*). SMS merupakan suatu layanan yang memungkinkan pengguna telepon selular untuk mengirimkan pesan singkat kepada pengguna telepon selular lainnya dengan cepat dan dengan biaya yang kecil.

SMS bekerja pada sistem nirkabel. Sistem nirkabel yang paling populer di dunia adalah GSM (*Global System for Mobile Communication*). Komponen yang digunakan oleh GSM dalam melakukan komunikasi SMS diantaranya:

a) *Mobile Station* merupakan perangkat *mobile* yang dapat melakukan pengiriman SMS.
b) ESME (*External Short Messaging Entities*) merupakan suatu perangkat yang dapat mengirimkan dan menerima SMS, pada umumnya menggunakan jaringan Internet.
c) BS (*Base Station*) menjadi antar muka antar jaringan komunikasi nirkabel dengan *mobile station.*
d) MSC (*Mobile Service Switching Center*) merupakan komponen utama pada komunikasi selular yang melakukan pengontrolan pertukaran informasi informasi yang terjadi pada jaringan selular.
e) Register-register yang diantaranya adalah HLR (*Home Location Register*) dan VLR (*Visitor Location Register*).
f) SMSC (*Short Message Service Center*) merupakan tempat di mana SMS disimpan sebelum dikirimkan ke tujuan.

Untuk lebih jelas mengenai jaringan SMS dapat dilihat pada **Gambar 1** yang di mana interaksi antara *mobile station* dan jaringan tersebut adalah melalui BS.



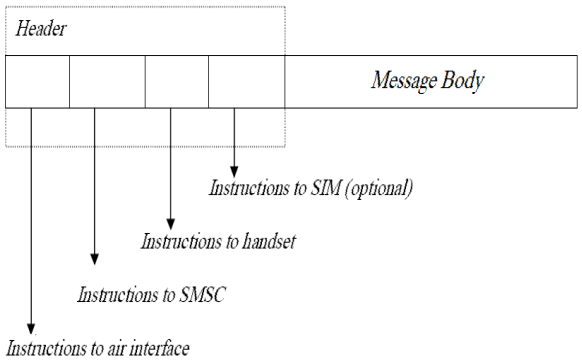
Gambar 1 Jaringan SMS [ENC05]

Celah keamanan terbesar pada komunikasi SMS adalah pesan yang dikirimkan akan disimpan pada SMSC, sehingga apabila terjadi serangan pada SMSC, maka pesan yang terkirim dapat terbaca. Salah satu cara menaggulangi celah tersebut adalah dengan melakukan enkripsi terhadap pesan yang dikirimkan. Dengan semakin majunya teknologi telepon selular, implementasi suatu algoritma enkripsi menjadi mungkin. Algoritma RC6 yang dirancang oleh Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, dan Y.L. Yin merupakan salah satu algoritma yang menjadi finalis kandidat untuk menjadi AES. Walaupun pada akhirnya algoritma ini tidak menang dalam kompetisi tersebut, namun algoritma ini cukup diakui kesederhanaannya sehingga menjadi mungkin diimplementasikan untuk enkripsi SMS pada telepon selular.

2. LANDASAN TEORI

2.1. Struktur Pesan SMS

Struktur pesan pada sebuah paket SMS dapat dilihat pada Gambar II-1 yang diadopsi dari [CLE03].



Gambar Error! No text of specified style in document.**-1 Struktur Pesan SMS**

Pada Gambar II-1 dapat terlihat bahwa pada sebuah paket pesan SMS terdiri dari *header* dan *body*. *Header* pesan terdiri dari instruksi-instruksi kepada komponen-komponen yang bekerja dalam jaringan SMS. Pada instruksi-instruksi tersebut, terdapat informasi yang diperlukan selama pengiriman pesan seperti informasi validitas pesan, dan informasi-informasi lainnya. Pada bagian *message body*, terdapat isi dari pengirim pesan yang akan dikirimkan.

Panjang isi pesan pada sebuah paket SMS berukuran maksimal 160 karakter, dimana setiap karakter memiliki panjang 7 bit. Beberapa aplikasi standar telepon selular dapat mendukung panjang pesan dengan karakter sepanjang 8 bit (panjang pesan maksimum 140 karakter) dan karakter yang lebih panjang lainnya seperti 16 bit, namun karakter sepanjang 8 bit dan 16 bit ini tidak didukung oleh semua aplikasi standar telepon selular. Pada umumnya

karakter sepanjang 8 bit dan 7 bit digunakan untuk menampilkan data seperti gambar dan simbol[PET07].

2.1. Algoritma RC6[RIV98]

Algoritma RC6 adalah suatu algoritma kriptografi *block cipher* yang dirancang oleh Ronald L. Rivest, Matt J.B. Robshaw, Ray Sidney, dan Yuqin Lisa Yin dari RSA Laboratories. Algoritma ini pada mulanya dirancang untuk menjadi AES (*Advance Encryption Standard*). Algoritma RC6 ini berhasil menjadi finalis dan menjadi kandidat kuat untuk menjadi AES walaupun pada akhirnya algoritma ini tidak terpilih menjadi AES melainkan algoritma *rinjdael*. Versi 1.1 dari RC6 mulai dipublikasikan pada tahun 1998. Dasar desain dari algoritma RC6 ini didasarkan pada pendahulunya yaitu algoritma RC5.

Algoritma RC6 merupakan algoritma dengan parameter penuh, algoritma RC6 dispesifikasikan dengan notasi RC6-*w/r/b.* Dimana *w* adalah ukuran dari *word* dalam bit, karena pada RC6 menggunakan 4 buah register maka *word* adalah ukuran blok dibagi 4. *r* adalah jumlah iterasi, dimana *r* tidak boleh negatif. Dan *b* adalah panjang kunci dalam *bytes.*

Pembentukan kunci internal yang akan digunakan pada proses enkripsi dan dekripsi dari algoritma RC6 menggunakan pembentukan kunci internal dari algoritma RC6. Proses untuk membangun kunci-kunci internal menggunakan dua buah konstanta yang disebut dengan "*magic constant*". Dua buah *magic constant* P_w dan Q_w tersebut didefinisikan sebagai berikut:

$P_w = Odd((e-2)2^w)$……..*(2.1)*

$Q_w = Odd((\emptyset-1)2^w)$……..*(2.2)*

Dimana :

e = 2.7182818284859…(basis dari logaritma natural)

$\emptyset$ = 1.618022988749…(golden ratio)

Odd (x) adalah integer ganjil terdekat dari x, jika x genap maka diambil integer ganjil setelah x.

Berikut adalah daftar *magic constant* pada beberapa panjang blok dalam heksadesimal:

$P_{16} = b7e1$
$Q_{16} = 9e37$
$P_{32} = b7e15163$
$Q_{32} = 9e3779b9$
$P_{64} = b7e151628aed2a6b$
$Q_{64} = 9e3779b97f4a7c15$

Dengan menggunakan dua buah *magic constant* tersebut, pembangunan kunci terdiri dari tiga tahap :

1. Konversi kunci rahasia dari *bytes* ke *words*

```
if c=0 then
        c←1
endif
for i←b-1 downto 0 do
        L[i/u]  ←  (L[i/u]<<<8)  +
        K[i]
endfor
```

Dimana c = pembulatan keatas(b/u) dan u = w/8

2. Inisialisasi *array* S

```
S[0] ← Pw
for i←0 to 2r+3 do
        S[i]←S[i-1]+ Qw
endfor
```

3. Mencampurkan L dan S

```
i←0
j←0
A←0
B←0
V←3*max(c,2r+4)
for index←1 to v do
        S[i]←(S[i]+A+B) <<< 3
        A←S[i]
        L[j]←(L[j]+A+B) <<< (A+B)
        B←L[j]
        i←(i+1)mod(2r+4)
        j←(j+1)mod c
endfor
```

Algoritma RC6 bekerja dengan empat buah register A,B,C,D yang masing-masing berukuran *w*-bit, register-register tersebut akan diisi oleh plainteks yang kemudian akan digunakan selama proses enkripsi dan setelah proses enkripsi berakhir isi dari register-register tersebut merupakan cipherteks.

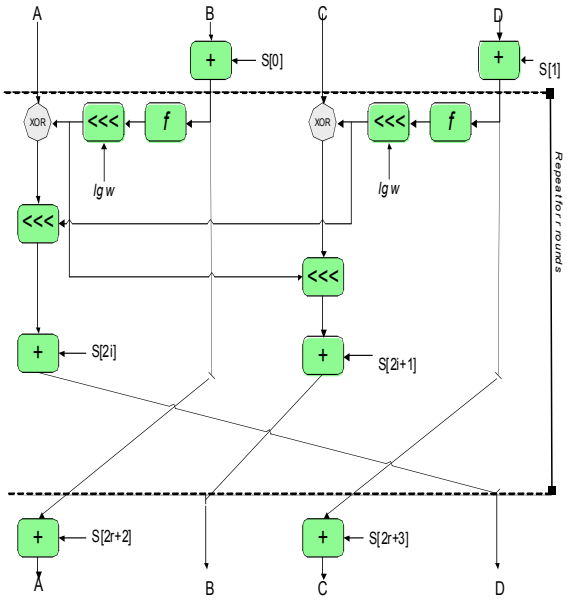
Proses enkripsi dan dekripsi algoritma RC6 menggunakan enam buah operasi dasar:

a+*b* = penjumlahan integer modulo 2^w
a - *b*=pengurangan integer modulo 2^w
a⊕*b*=operasi bitwise exclusive-or sebesar *w*-bit *words*
*a***b* = perkalian integer modulo 2^w
a<<<*b*=rotasi sejumlah *w*-bit *word* ke kiri sebanyak jumlah yang diberikan oleh *least sifnificant* lg *w* bit dari b
a>>>*b*=rotasi sejumlah *w*-bit *word* ke kanan sebanyak jumlah yang diberikan oleh *least sifnificant* lg *w* bit dari b
Dimana lg *w* adalah logaritma basis dua dari *w*.

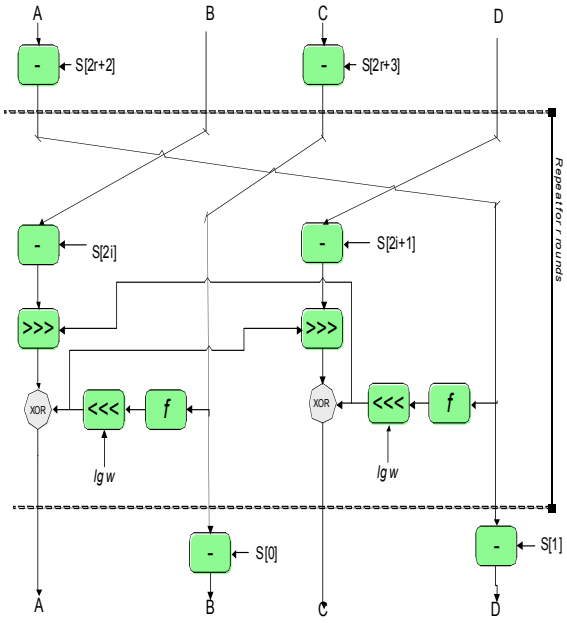
Proses enkripsi algoritma RC6 adalah sebagai berikut:

```
Prosedure Enkripsi
(Input :Plainteks dalam A,B,C,D
        r : integer (jumlah rotasi)
        S[0..2r+3] : kunci internal
Output :Cipherteks dalam A,B,C,D)
Kamus
        u : integer
        t : integer
Algoritma
        B ← B + S[0]
        D ← D + S[1]
        for i ← 1 to r do
          t ← (B * (2B + 1))<<<lg w
          u ← (D * (2D + 1))<<<lg w
          A ← ((A ⊕ t)<<<u) + S[2i]
          C ← ((C ⊕ u)<<<t) + S[2i+ 1]
          (A,B,C,D) ← (B,C,D,A)
        endfor
        A ← A + S[2r + 2]
        C ← C + S[2r + 3]
```

Atau dapat dilihat pada **Gambar 2** dengan *f(x)=x*(2x+1)*.



Gambar 2 Diagram Enkripsi RC6



Gambar 3 Proses Dekripsi RC6

Proses dekripsi dari algoritma RC6 adalah sebagai berikut:

```
Prosedure Dekripsi
(Input :Cipherteks dalam A,B,C,D
       r : integer (jumlah rotasi)
       S[0..2r+3] : kunci internal
       Output :Plainteks dalam A,B,C,D)
Kamus
       u : integer
       t : integer
Algoritma
       C ← C - S[2r + 3]
       A ← A - S[2r + 2]
       for i ← r downto 1 do
         (A,B,C,D) ← (D,A,B,C)
         u ← (D * (2D + 1))<<<lg w
         t ← (B * (2B + 1))<<<lg w
         C ← ((C - S[2i+ 1])>>>t) ⊕ u
         A ← ((A - S[2i])>>>u) ⊕ t
       endfor
       D ← D - S[1]
       B ← B - S[0]
```

Atau dapat dilihat pada **Gambar 3** dengan *f(x)=x*(2x+1)*.

3. ANALISIS MASALAH

3.1. Implementasi Algoritma RC6

Pada tugas akhir ini algoritma RC6 yang diimplementasikan memiliki spesifikasi sebagai berikut:

RC6 –32/r/b

Dimana panjang blok adalah 32 bit dikali 4, jumlah rotasi akan dapat beragam dan begitu pula dengan panjang kunci.

Mode yang akan diterapkan pada perangkat lunak adalah mode ECB, mode ini adalah mode yang paling sederhana dan sering digunakan. Dalam *block cipher* dibutuhkan metode pemrosesan blok dan mode ECB yang memproses setiap blok secara independen akan memerlukan jumlah memori yang sedikit dan waktu pemrosesan yang singkat.

Karakter yang dapat digunakan pada SMS beragam, sebuah karakter dapat memiliki panjang 7 bit, 8 bit atau 16 bit, sebuah pesan tidak dapat memiliki karakter dengan panjang yang beragam, hal ini harus diperhatikan dalam melakukan perancangan algoritma enkripsi. Jika panjang karakter yang digunakan menggunakan panjang 7 bit, maka akan menimbulkan masalah karena pada algoritma RC6 terdapat "*lg w*" dimana merupakan logaritma basis dua dengan *w* adalah panjang *word*, jika yang digunakan kerakter dengan panjang 7 bit, maka panjang *word* akan menjadi kelipatan 7 sehingga tidak akan ditemukan bilangan bulat dari "*lg w*". Atas dasar pertimbangan tersebut, dalam implementasi yang akan dilakukan karakter yang akan digunakan adalah karakter menggunakan karakter dengan panjang 8 bit.

3.2. Analisis Penerapan Enkripsi SMS

Pada tugas akhir ini, aplikasi yang akan dibangun merupakan aplikasi pengiriman dan penerimaan pesan yang berdiri sendiri. Hal tersebut berdasarkan pertimbangan dimana aplikasi SMS standar tiap jenis telepon selular tidaklah sama, panjang sebuah karakter dapat beragam dan kemampuan untuk melakukan konkatinasi tidak dimiliki oleh semua jenis telepon selular dan juga tidak semua aplikasi pengiriman SMS mengirimkan pesan dalam bentuk *binary*.

Penggunaan nomor *port* pada sebuah aplikasi pengiriman dan penerimaan SMS dapat berdiri sendiri dan tidak mengganggu aplikasi standar yang terdapat pada telepon selular. Penerimaan pesan akan melalui nomor *port* tersebut dan pengiriman pesan akan selalu ditujukan pada nomor *port* tersebut. Nomor *port* yang digunakan tentunya akan menggunakan nomor *port* yang belum digunakan oleh aplikasi-aplikasi standar pada telepon selular. Pemakaian nomor *port* ini akan menyebabkan panjang pesan berkurang karena informasi nomor *port* tersebut akan dikirimkan. Pemakaian nomor *port* ini juga akan menyebabkan aplikasi dapat berdiri sendiri namun tidak akan dapat menerima pesan jika diimplementasikan pada telepon selular yang menggunakan kartu SIM berjenis CDMA. Nomor *port* tersebut dibawa pada UDH (*User Data Header*) pada paket data SMS, yang dimana UDH tersebut tidak terdapat pada paket data SMS pada CDMA.

Pembangunan aplikasi SMS yang berdiri sendiri akan memiliki kekurangan dimana aplikasi tidak akan dapat menerima pesan jika diimplementasikan pada telepon selular CDMA yang menyebabkan jenis telepon selular yang dapat digunakan menjadi terbatas pada telepon selular GSM, namun jika aplikasi yang dibangun bukan merupakan aplikasi yang berdiri sendiri atau menggunakan fungsi-fungsi dari aplikasi standar sebuah telepon selular, maka kompatibilas aplikasi akan lebih terbatas karena telepon selular yang dapat digunakan hanya akan terbatas pada aplikasi standarnya, jika aplikasi standarnya berbeda maka aplikasi yang dibangun tidak akan dapat digunakan dan pada umumnya hanya sedikit sekali jenis telepon selular yang menggunakan aplikasi standar yang sama. Atas dasar pertimbangan tersebut, aplikasi yang dibangun akan ditujukan untuk pengguna GSM.

Dalam implementasi yang akan dilakukan, jika sebuah pesan telah terenkripsi, maka, dalam pengiriman pesan, pesan yang dikirim berupa pesan *binary* yang terdiri dari *byte-byte* hasil enkripsi.

3.2. Analisis Dampak Sistem

Berikut adalah hasil analisis dampak aplikasi yang dibangun:

1. Dampak perangkat lunak terhadap sistem telepon selular

Perangkat lunak yang akan dibangun akan berdiri sendiri, oleh karena itu perangkat lunak yang akan dibangun tidak melakukan komunikasi atau berinteraksi dengan aplikasi yang sudah terdapat pada telepon selular. Pada dasarnya, sebuah telepon selular hanya memiliki sebuah saluran untuk melakukan pengiriman SMS, oleh karena itu ketika perangkat lunak yang akan dibangun sedang melakukan pengiriman SMS, maka selama pengiriman tersebut, aplikasi SMS lain tidak dapat melakukan pengiriman SMS, begitu pula sebaliknya. Hal yang sama terjadi juga pada penerimaan SMS, walaupun menggunakan nomor *port*, namun pada dasarnya saluran penerimaan SMS pada telepon selular hanya satu, nomor *port* tersebut hanya digunakan untuk menandai aplikasi yang akan menerima pesan. SMS yang dikirimkan oleh perangkat lunak yang akan dibangun akan diterima oleh perangkat lunak yang sama, jika telepon selular yang dituju tidak memiliki perangkat lunak tersebut, maka SMS akan masuk ke dalam aplikasi SMS standar yang dimiliki oleh telepon selular tersebut.

2. Dampak keamanan oleh perangkat lunak

Dengan dienkripsinya SMS yang dikirimkan, maka serangan berjenis *man-in-the-middle attack* yang terjadi ketika pesan berada pada jaringan SMS dapat dihindarkan. SMS yang dikirimkan oleh pengirim akan berhenti pada jaringan SMS seperti MSC, pada saat ini, penyerang dapat melihat pesan yang dikirmkan, penyerang akan mudah memilih pesan untuk dibaca, karena nomor pengirim akan terdapat pada pesan yang dikirimkan, namun dengan dienkripsinya isi pesan, penyerang tidak dapat membaca pesan tersebut. Kerahasiaan pun akan terjaga apabila terjadi salah kirim, karena tanpa masukkan kunci yang benar pesan tidak akan terbaca.

3. Perbandingan dengan aplikasi SMS standard

Jika dibandingkan dengan aplikasi SMS standar, perangkat lunak yang akan dibangun akan memberikan keuntungan berupa keamanan. Pesan yang dikirimkan oleh perangkat lunak yang akan dibangun akan terenkripsi sehingga sulit untuk dibaca. Namun perangkat lunak yang akan dibangun akan memiliki kekurangan yaitu, pesan akan cenderung membesar, ada kemungkinan sebuah pesan berubah menjadi dua buah pesan setelah dienkripsi.

3.3. Implementasi

Dalam melakukan implementasi, penulis menggunakan bahasa pemrograman java, dengan lingkungan pembangunan sebagai berikut :

Perangkat komputer yang digunakan untuk melakukan implementasi memiliki spesifikasi sebagai berikut:

1. Prosessor Intel Core Duo 1.8 GHz
2. RAM 1 GB
3. Hard Disk 80 GB
4. Perangkat masukkan keyboard dan tetikus
5. Perangkat keluaran monitor

Adapun perangkat lunak yang digunakan dalam melakukan implementasi adalah sebagai berikut:

1. Sistem operasi Windows XP *Service Pack* 2
2. Netbeans IDE 6.0.1
3. Mobility pack for Netbeans IDE
4. Sun Java Wireless Toll Kit 2.5.2

Pada tugas akhir ini, perangkat lunak yang dibangun memiliki batasan sebagai berikut:

1. Perangkat lunak tidak dapat melakukan akses ke memory di dalam kartu SIM.
2. Perangkat lunak yang dibangun dapat dijalankan pada telepon selular yang dapat mendukung aplikasi berbasis java dengan spesifikasi MIDP 2.0 dan CLDC 1.1 menggunakan kartu GSM.

3.PENGUJIAN

Pengujian yang dilakukan dibagi menjadi tiga bagian yaitu pengujian performansi perangkat lunak, pengujian enkripsi dan dekripsi, dan pengujian pengiriman dan penerimaan pesan. Pengujian ini dilakukan pada telepon selular Nokia 9300i yang memiliki memory *internal* 80 MB dan *memory card* 128 MB.

Berdasarkan hasil pengujian yang dilakukan, hasil dari pengujian fitur enkripsi dan dekripsi perangkat lunak pada lingkungan telepon selular berjalan dengan cukup cepat. Semakin besar jumlah rotasi yang digunakan, waktu yang diperlukan untuk enkripsi dan dekripsi cenderung semakin besar.

Keamanan dapat terjaga terbukti jika kunci yang dimasukkan salah atau nomor tujuan tidak memiliki aplikasi untuk dekripsi, maka pesan terenkripsi yang diterima tidak akan dimengerti maksudnya.

Melalui hasil pengujian yang dilakukan pada telepon selular, dapat terlihat bahwa perangkat lunak berjalan dengan baik dan jika nomor tujuan menggunakan perangkat lunak yang sama, pesan dapat disampaikan dengan baik, dapat diketahui bahwa implementasi algoritma RC6 untuk komunikasi melalui media SMS dapat direalisasikan dengan baik.

4. KESIMPULAN

Dari keseluruhan isi makalah ini, dapat diambil kesimpulan sebagai berikut:

1. Sebuah perangkat lunak yang mengimplementasikan suatu algoritma kriptografi kunci privat untuk enkripsi SMS telah berhasil dibangun. Perangkat lunak yang dibangun tersebut dapat melakukan pengiriman pesan dan penerimaan pesan terenkripsi tersebut dengan baik. Perangkat lunak tersebut menggunakan algoritma RC6 untuk enkripi SMS. Perangkat lunak tersebut dapat ditanamkan pada telepon selular dan dibangun dengan menggunakan bahasa pemrograman java.
2. Penerapan algoritma kunci privat untuk enkripsi SMS pada telepon selular dapat meningkatkan keamanan. Pesan yang terenkripsi tidak akan dapat dibaca jika tidak didekripsi dengan menggunakan kunci yang benar, sehingga orang yang tidak mengetahui kunci yang sebenenarnya tidak dapat membaca pesan yang dikirimkan.
3. Algoritma RC6 dapat diimplementasikan dengan baik untuk melakukan enkripsi SMS yang bekerja pada jaringan GSM dengan mengirimkan pesan yang berbentuk *binary*.
4. Kekurangan dari implementasi algoritma RC6 untuk enkripsi SMS adalah pesan yang dikirimkan menjadi lebih besar karena harus bekerja pada 8 bit dan dibutuhkan *padding* untuk memenuhi panjang blok.
5. Semakin besar jumlah rotasi pada algoritma RC6, maka tingkat keamanan akan semakin baik, namun waktu yang diperlukan untuk melakukan enkripsi dan dekripsi akan semakin besar.

5. SARAN

1. Agar pesan terenkripsi yang dikirimkan memiliki panjang pesan yang sama dengan plainteks yang ditulis oleh pengirim, sebaiknya diterapkan sebuah algoritma kompresi untuk melakukan kompresi pesan sehingga.
2. Algoritma enkripsi yang diterapkan sebaiknya dapat menangani panjang karakter yang memiliki panjang 7 bit untuk melakukan enkripsi SMS. Pada dasarnya panjang karakter pada SMS adalah 7 bit oleh karena itu agar SMS yang dikirimkan tidak mengalami penambahan panjang sebaiknya digunakan suatu algoritma enkripsi yang mampu menangani karakter sepanjang 7 bit.

DAFTAR PUSTAKA

[ENC05] Enck, William., Patrick Traynor, Patrick McDaniel, Thomas La Porta. (2005). Exploiting Open Functionality in SMS-Capable Cellular Networks. http://www.smsanalysis.org diakses pada Oktober 2007.

[HAL07] Halim, Abdul. (2007) Penerapan Kriptografi Kunci-Simetri dan Asimetri untuk Mengamankan Multimedia Messaging Service (MMS). Tugas Akhir Mahasiswa Institut Teknologi Bandung.

[KHA05] Khan, Atique Ahmed. (2005). Security & Vulnerability Analysis of Wireless Messaging Protocols & Application. http://www.securitydocs.com diakses pada Oktober 2007.

[MOU92] Mouly, Michel., Marie-Bernadette Pautet. (1992). The GSM System for *Mobile* Communication.

[NEC00] Nechvatal, James., Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback (2000) Report on the Development of the Advanced Encryption Standard (AES). http://csrc.nist.gov diakses pada Oktober 2007.

[CLE03] Clements.T. (2003). SMS–Short but Sweet. Sun Microsystems: http://developers.sun.com/techtopics/mobility/midp/articles/sms/ diakses pada Oktober 2007.

[JSR02] JSR 120 Expert Group. (2002). Wireless Messaging API (WMA) for Java™ 2 Micro Edition Reference Implementation. Sun Microsystem Inc.

[MEN96] Menezes, A., P. van Oorschot, and S. Vanstone.(1996) Handbook of Applied Cryptography, CRC Press: http://www.cacr.math.uwaterloo.ca/hac

[MUN06] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi. Bandung.

[PET07] Pettersson, Lars. SMS Message and The PDU Format: http://www.dreamfabric.com/sms/ diakses pada bulan November 2007.

[RIV98] Rivest, L. Ronald., M.J.B. Robshaw., R. Sidney., Y.L. Yin. (1998) The RC6™ Block Cipher. http://rsa.com diakses pada Oktober 2007.