IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI DAN DEKRIPSI SMS PADA HANDPHONE BERBASIS JAVA
IMPLEMENTATION OF RC6 ALGORITHM FOR SMS ENCRYPTION AND DECRYPTION IN JAVA-BASED HANDPHONE

Ella Evelin[1], Ari Moesriami Barmawi[2], Msc.[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

---

Abstrak

Saat ini, SMS mungkin merupakan kebutuhan yang penting dalam berkomunikasi. Dengan adanya fasilitas SMS, maka dengan cepat seseorang dapat menyampaikan berita/kabar, namun komunikasi melalui media SMS bukanlah komunikasi point-to-point, melainkan melalui jaringan SMS. Pada jaringan SMS tersebutlah, keamanan pesan sangatlah terancam untuk dibaca oleh orang yang tidak bertanggung jawab, maka perlu dilakukan proses enkripsi dan dekripsi SMS.

Proses enkripsi dan dekripsi terhadap SMS yang diterima maupun dikirim dilakukan pada tugas akhir ini. Adapun pengimplementasian enkripsi dan dekripsi SMS menggunakan algoritma RC6. Algoritma RC6 memiliki waktu pemprosesan enkripsi dan dekripsi yang cenderung lebih cepat dan memiliki kelebihan dalam bidang data dependent rotation dalam enkripsi.

Tugas akhir ini menghitung dan menganalisis pengujian waktu enkripsi dan dekripsi pesan. Pengujian dilakukan dengan menggunakan data jumlah round, jumlah karakter, dan panjang kunci yang beragam. Dari hasil pengujian didapatkan bahwa semakin besar jumlah round, jumlah karakter, dan panjang kunci, maka semakin besar juga waktu enkripsi dan dekripsi pesan yang dibutuhkan.

Kata Kunci : enkripsi, dekripsi, algoritma RC6, round, panjang kunci, waktu enkripsi dan dekripsi

---

Abstract

Currently, the SMS may be an important requirement in communication. With the SMS facility, then quickly a person can submit news , but the communication through the medium of SMS is not a communication point-to-point, through the SMS network. In SMS network, the security message is threatened to be read by people who are not responsible, it is necessary to process the encryption and decryption SMS.

The process of encryption and decryption of the SMS received and sent carried out in this final. The implementation of encryption and decryption algorithms SMS using RC6. RC6 algorithm has a processing time of encryption and decryption which tend to more quickly and have advantages in the field of data dependent rotation in encryption.

This final assigment counted and analyzed about message encryption and decryption time. Tests carried out by using the data the number of round, the number of characters, and a variety of key length. From the test results showed that the greater the number of round, the number of characters, and key length, the greater also encrypt and decrypt messages when needed.

Keywords : encryption, decryption, RC6 Algorithm, round, key length, encryption and decryption time

---

1. Pendahuluan

Bab pendahuluan membahas tentang hal-hal yang melatarbelakangi pemilihan judul tugas akhir, masalah yang diangkat dalam tugas akhir, batasan-batasan masalah yang merupakan ruang lingkup dari tugas akhir, tujuan yang dicapai dari pembuatan tugas akhir, hipotesa awal dari tugas akhir, dan metode penyelesaian yang dibagi menjadi dua yaitu metode penyelesaian tugas akhir dan metode penyelesaian masalah, serta sistematika penulisan.

1.1 Latar Belakang

SMS (*Short Message Service*) merupakan suatu layanan yang diberikan oleh telepon selular kepada para pelanggannya untuk melakukan komunikasi melalui pengiriman pesan singkat dengan biaya yang murah. Saat ini, SMS mungkin merupakan kebutuhan yang penting dalam berkomunikasi. Misalnya saja ketika seseorang ingin menyampaikan berita/kabar kepada temannya yang tinggalnya jauh, maka dengan adanya fasilitas SMS tersebut dengan cepat seseorang dapat menyampaikan berita/kabar. Maka dapat dikatakan bahwa komunikasi melalui SMS tidak mengenal jarak dan waktu. Komunikasi melalui media SMS bukanlah komunikasi *point-to-point*, dimana 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. Maka, tantangannya adalah bagaimana mengamankan SMS yang dikirimkan tersebut?

Saat ini kriptografi yang digunakan untuk mengamankan SMS adalah algoritma RSA (seperti pada Tugas Akhir "Implementasi Algoritma RSA dalam Enkripsi dan Dekripsi SMS di *Handphone* Berbasis Java" dibuat oleh Chiara Alamanda, dengan NIM 113040320, Institut Teknologi Telkom). Algoritma RSA memiliki kekurangan dalam hal waktu enkripsi dan dekripsi pesan.

Dengan melihat adanya kekurangan pada algoritma RSA, maka pada tugas akhir ini dibuatlah metode pengamanan SMS yang baru.

Kriptografi yang digunakan untuk mengamankan SMS yang juga pernah digunakan adalah algoritma RC6 (pada tugas akhir "Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler" oleh Rangga Wisnu Adi Permana, dengan NIM 135 04 036, Institut Teknologi Bandung) [12]. Adapun permasalahan yang terdapat pada tugas akhir tersebut [12] adalah bahwa tugas akhir tersebut belum menganalisa tentang waktu enkripsi dan dekripsi berdasarkan round dan panjang kunci, brute-force attack, kriptanalisis differensial, data dependent rotation, dan kunci yang digunakan tidak dapat diubah (statis) tanpa melakukan pertukaran kunci secara offline.

1.2 Perumusan Masalah

Pada sub bab latar belakang telah diuraikan hal-hal yang melatarbelakangi pemilihan tugas akhir ini, sehingga berdasarkan latar belakang yang ada diangkat masalah berikut :

1. Beberapa algoritma enkripsi seperti RSA membutuhkan waktu enkripsi dan dekripsi yang relatif lama sehingga kurang efisien jika digunakan untuk mengamankan SMS.
2. Algoritma RC6 yang pernah digunakan untuk enkripsi SMS [12] masih menggunakan kunci statis dan kinerjanya belum dianalisis secara komprehensif.

1.3 Batasan Masalah

Dalam pembuatan tugas akhir ini terdapat beberapa batasan masalah. Batasan masalah yang ada bertujuan untuk menjelaskan ruang lingkup tugas akhir ini. Berikut batasan masalah dalam tugas akhir ini adalah :

1. Jenis SMS yang digunakan adalah SMS pribadi.
2. Isi pesan yang dienkripsi berupa teks.
3. Aplikasi menangani masalah ketahanan algoritma terhadap serangan.
4. Aplikasi tidak menangani penghapusan database *secret key* dari RC6.
5. Aplikasi menangani penyimpanan SMS yang sebelumnya dikirim maupun diterima (menangani *inbox* maupun *outbox*).
6. Aplikasi yang dibangun ditujukan untuk pengguna GSM saja.
7. Karakter yang digunakan adalah karakter dengan panjang 8 bit.
8. Aplikasi yang dibangun adalah aplikasi yang berdiri sendiri (terpisah dari aplikasi SMS standar yang dimiliki oleh telepon selular yang menjadi objek implementasi).

1.4 Tujuan

Dengan diuraikannya rumusan masalah pada sub bab sebelumnya, maka melalui tugas akhir ini terdapat tujuan yang dicapai. Dengan adanya tujuan, maka diharapkan tugas akhir ini nantinya dapat berguna untuk setiap orang yang memerlukannya. Adapun tujuan yang dicapai dari tugas akhir ini adalah mencari metode pengamanan SMS yang membutuhkan waktu enkripsi dan dekripsi yang lebih rendah dari waktu enkripsi dan dekripsi yang dibutuhkan pada metode pengamanan SMS lain seperti dengan algoritma RSA.

1.5 Hipotesa Awal

Pada saat ini, ada beberapa algoritma yang dapat melakukan teknik enkripsi dan dekripsi, contohnya saja algoritma RSA (*Rivest Shamir Adleman*), algoritma Rijndael atau algoritma AES (*Advanced Encryption Standard*), algoritma RC6 (*Rivest Cipher* 6). Algoritma RSA termasuk algoritma asimetri, dimana kelemahannya adalah proses enkripsi dan dekripsinya lambat dikarenakan pada algoritma RSA menggunakan faktorisasi serta bilangan yang digunakan pada algoritma RSA hanyalah bilangan prima saja. Algoritma Rijndael termasuk algoritma simetri,

dimana kelemahannya adalah pada bidang *data dependent rotation* dalam enkripsi. Dengan mengacu pada kelemahan yang ada pada algoritma RSA dan algoritma Rijndael, maka dipilihlah algoritma RC6 dalam tugas akhir ini untuk mengatasi kelemahan dari kedua algoritma tersebut. Algoritma RC6 memiliki waktu pemprosesan enkripsi-dekripsi yang cenderung lebih cepat daripada algoritma RSA dan memiliki kelebihan dalam bidang *data dependent rotation* dalam enkripsi dibandingkan dengan algoritma Rijndael.

Dalam pertukaran kunci bisa terjadi serangan apalagi mengingat bahwa kunci RC6 adalah algoritma kunci simetris dimana hanya ada satu kunci yang digunakan untuk enkripsi dan dekripsi pesan, sehingga kunci RC6 akan dienkripsi lagi dengan sebuah metode, dimana hal ini dilakukan dengan tujuan keamanan terhadap kunci.

Jadi, pada tugas akhir ini dibangun aplikasi enkripsi dan dekripsi SMS untuk meningkatkan keamanan pesan dengan melakukan enkripsi dan dekripsi terhadap pesan yang dikirimkan menggunakan algoritma RC6. Adapun perbedaan mendasar pada tugas akhir ini dengan tugas akhir "Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler" [12] adalah pada segi kunci, dimana penggunaan kunci pada tugas akhir ini adalah dinamis, sedangkan pada tugas akhir "Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler" [12] adalah statis.

1.4 Metodologi Penyelesaian

Tugas akhir ini dibuat dengan melakukan beberapa tahapan, dimana setiap tahapannya memiliki peranan masing-masing serta antar tahapan memiliki keterkaitan/keterhubungan. Adapun metode penyelesaiannya dibagi atas dua yaitu metodologi penyelesaian tugas akhir dan metodologi penyelesaian masalah. Berikut uraian dari kedua metodologi tersebut.

1.6.1 Metodologi Penyelesaian Tugas Akhir

Metodologi penyelesaian tugas akhir berisi uraian dari setiap tahapan mengenai apa yang dilakukan dalam setiap tahapan. Berikut uraian dari setiap tahapan dalam penyelesaian tugas akhir :

1. Studi Literatur
   Tahap studi literatur bertujuan untuk meningkatkan pemahaman terhadap setiap materi-materi yang digunakan dalam tugas akhir ini, dimana yang dipelajari adalah mengenai kriptografi (sejarah kriptografi, definisi kriptografi, tujuan kriptografi, kunci simetri dan kunci asimetri, landasan matematika yang digunakan dalam kriptografi), serangan terhadap kriptografi khususnya untuk enkripsi-dekripsi SMS, algoritma RC6 dan J2ME dari buku, *website*, maupun artikel-artikel lain yang menunjang tugas akhir ini.
2. Analisis dan Perancangan Aplikasi
   Pada tahap ini dilakukan analisis kebutuhan dari aplikasi enkripsi-dekripsi SMS yang dibuat dalam tugas akhir ini, setelah itu membuat desain aplikasi dengan menggunakan teknik berorientasi objek, yaitu *Use Case Diagram*, *Class Diagram*, *Sequence Diagram*, dan *Deployment Diagram*.

3. Implementasi Aplikasi
   Pada tahap ini dilakukan implementasi aplikasi sesuai dengan analisis dan perancangan aplikasi yang telah dibuat sebelumnya.
4. Pengujian dan Analisis Aplikasi
   Setelah dilakukan implementasi aplikasi, maka dilakukan pengujian terhadap aplikasi enkripsi dekripsi SMS dan selanjutnya melakukan analisis terhadap aplikasi, dimana pada tahap ini dilihat apakah aplikasi enkripsi dekripsi SMS yang dibuat sudah sesuai dengan desain yang dibuat dan sesuai dengan kebutuhan.
5. Pengambilan Kesimpulan dan Pembuatan Laporan Tugas Akhir
   Pada tahap ini dilakukan pengambilan kesimpulan terhadap hasil pengujian dan analisis terhadap aplikasi enkripsi dekripsi SMS yang telah dilakukan pada tahap sebelumnya, dan juga dilakukan pembuatan laporan tugas akhir.

1.6.2 Metodologi Penyelesaian Masalah

Selain ada metodologi penyelesaian tugas akhir, ada juga metodologi penyelesaian masalah. Metodologi penyelesaian masalah bertujuan untuk menguraikan tahapan-tahapan yang dilakukan dalam menyelesaikan masalah, dimana tahapan-tahapannya tersebut dapat dikatakan merupakan apa yang ada pada aplikasi yang dibuat. Pada paragraf selanjutnya akan dijelaskan mengenai tahapan-tahapan penyelesaian masalah.

Yang pertama kali dilakukan adalah menentukan fungsionalitas yang ada dalam aplikasi yang dibuat, dimana fungsionalitasnya adalah sebagai berikut:

- fungsi *login*
- fungsi untuk mengubah password
- fungsi generate, enkripsi, dekripsi kunci RC6
- fungsi enkripsi, dekripsi pesan
- fungsi untuk menyimpan SMS yang dikirim maupun yang diterima (fungsi *inbox* dan *outbox*)

Setelah fungsionalitas ditentukan, maka dilakukanlah pembangunan *source code* pada NetBeans IDE 6.8, kemudian dari fungsionalitas yang telah dibuat, dilakukan pengujian terhadap fungsionalitas dan sistem. Pengujian terhadap fungsionalitas dilakukan dengan J2ME Wireless Toolkit 2.2, sedangkan pengujian terhadap sistem dilakukan dengan melakukan serangan (*attack*) terhadap sistem yang bertujuan untuk menguji ketahanan algoritma RC6 terhadap serangan.

1.5 Sistematika Penulisan

Dalam penyusunan buku tugas akhir ini menggunakan sistematika penulisan, dimana bertujuan agar penulisan tugas akhir lebih terarah dan tersusun dengan baik. Adapun sistematika penulisan di dalam tugas akhir ini dibagi atas enam bab, yaitu pendahuluan, landasan teori, perancangan sistem, implementasi, pengujian dan analisis, kesimpulan dan saran.

Pada bab pendahuluan dibahas mengenai latar belakang pembuatan tugas akhir, perumusan masalah, batasan masalah, tujuan, hipotesa awal, metodologi penyelesaian masalah dan sistematika penulisan.

Setelah bab pendahuluan, pada bab kedua yaitu bab landasan teori dikemukakan berbagai teori yang mendukung penyusunan tugas akhir, antara lain meliputi teori tentang kriptografi, tujuan kriptografi, kunci simetri dan asimetri, serangan terhadap kriptografi, algoritma RC6, algoritma yang digunakan untuk mengenkripsi dan mendekripsi kunci RC6.

Bab selanjutnya adalah bab perancangan sistem, dimana pada bab ini dijelaskan tentang proses analisa dan perancangan aplikasi enkripsi dekripsi SMS yang dibuat.

Setiap kebutuhan dan perancangan sistem kemudian diimplemetasikan, sehingga pada bab keempat berisi hasil (*printscreen*) dari setiap bagian menu yang ada di program aplikasi enkripsi dekripsi dengan menggunakan algoritma RC6, dan menggambarkan proses pengujian.

Setelah dilakukan implementasi, maka pada bab 5 dilanjutkan dengan tahapan pengujian. Pengujian yang dilakukan adalah pengujian terhadap fungsionalitas dan pengujian terhadap waktu enkripsi dan dekripsi pesan dengan menggunakan algoritma RC6, dimana setiap pengujian memiliki skenario pengujian. Setelah itu dilakukan analisis terhadap setiap hasil skenario pengujian dan juga serangan, serta *data dependent rotation*.

Pada bab terakhir yaitu bab kesimpulan dan saran dikemukakan kesimpulan dari apa yang didapatkan terhadap setiap proses yang dilakukan pada aplikasi dan terutama algoritma RC6 itu sendiri dan juga terdapat saran pengembangan dari tugas akhir yang berfungsi untuk menjadi bahan masukan jika tugas akhir ini dikembangkan.

Kesimpulan dan Saran

6.1 Kesimpulan

Tugas akhir ini melakukan perbaikan mendasar dari tugas akhir "Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler" [12] pada segi kunci, dimana penggunaan kunci pada tugas akhir ini adalah dinamis, sedangkan pada tugas akhir "Implementasi Algoritma RC6 untuk Enkripsi SMS pada Telepon Seluler" [12] adalah statis.

Semakin besar jumlah *round*, maka semakin besar pula waktu yang dibutuhkan untuk enkripsi dan dekripsi pesan. Selain itu kenaikan waktu juga dipengaruhi oleh jumlah *round* yang digunakan dan panjang karakternya, sehingga semakin besar jumlah *round* dan jumlah karakter yang digunakan, maka semakin besar pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pesan.

Dari pengujian yang dilakukan dapat disimpulkan bahwa waktu enkripsi dan dekripsi pesan dengan menggunakan kunci RSA lebih besar dari waktu enkripsi dan dekripsi pesan dengan menggunakan kunci RC6. Hal tersebut dikarenakan algoritma RSA menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.

Dalam pengujian terdapat beberapa grafik (seperti gambar 5.1, gambar 5-4, gambar 5-7, gambar 5-12) yang mengalami kenaikan yang signifikan. Hal tersebut dikarenakan adanya pengaruh dari pemakaian memori untuk proses enkripsi dan dekripsi pesan.

Dalam hal *exhaustive key search attack* atau *brute force attack* dapat disimpulkan bahwa semakin panjang kunci, maka *exhaustive key search* semakin sulit untuk dilakukan atau dengan kata lain waktu *brute force* yang dibutuhkan terus meningkat seiring dengan meningkatnya jumlah kemungkinan kunci dan waktu dekripsi pesan.

Operasi perkalian 32 bit adalah salah satu operasi yang ada pada algoritma RC6, dimana operasi perkalian tersebut digunakan untuk menghitung jumlah bit yang dirotasi sehingga konsep data *dependent rotation* dapat dengan lebih sempurna diimplementasikan pada algoritma RC6 daripada algoritma Rijndael.

6.2 Saran

Dalam tugas akhir ini, metode pengamanan yang digunakan untuk mengenkripsi kunci RC6 adalah kunci RSA, maka daripada itu untuk penelitian lebih lanjut mungkin dapat digunakan algoritma yang lain (dalam hal ini adalah algoritma kriptografi kunci asimetri) yang lebih baik dari algoritma RSA, sehingga dapat dilihat apakah waktu enkripsi dan dekripsi RC6 akan cenderung lebih cepat dari algoritma yang lain yang akan digunakan untuk penelitian lebih lanjut tersebut.

Penyimpanan SMS (*inbox* dan *outbox*) dalm tugas akhir ini adalah berdiri sendiri, dan untuk penelitian lebih lanjut *inbox* dan *outbox* yang digunakan dapat digabung dengan *inbox* dan *outbox* yang sudah terdapat pada *handphone*.

Daftar Pustaka

[1] Bu'ulo, Roland L. *Perbandingan Algoritma Block Cipher RC5 dan RC6*.

[2] Clements,T. 2003. *SMS - Short But Sweet*. Sun Microsystems: http://developers.sun.com/techtopics/mobility/midp/articles/sms diakses pada 31 Agustus 2009.

[3] Contini, S., Rivest, R.L., Robshaw, M.J.B, Yin, Y.L. 1998. *The Security of RC6™ Block Cipher*. RSA Laboratories.

[4] Enck, William., Patrick Traynor, Patrick MCDaniel, Thomas La Porta. 2005. *Exploiting Open Functionality in SMS-Capable Cellular Networks*. http://www.smsanalysis.org diakses pada 31 Agustus 2009.

[5] Indra. *Mobile Programming*.

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

[7] Munir, Rinaldi. *Algoritma Brute Force Bagian 2*.

[8] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika Bandung.

[9] Petterson, Lars. *SMS Message and The PDU Format*: http://www.dreamfabric.com/sms diakses pada 31 Agustus 2009.

[10] Rivest, L. Ronald., M.J.B. Robshaw., R. Sidney., Y.L. Yin. 1998. *The RC6™ Block Cipher*. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.66.4235 diakses pada 1 Agustus 2009.

[11] Rudianto. *Analisis Keamanan Algoritma Kriptografi RC6*.

[12] Wisnu Adi Permana, Rangga. *Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular*.