Tersedia di http://jtsiskom.undip.ac.id (10 Agustus 2016)
DOI: 10.14710/jtsiskom.4.3.2016.450-453
Jurnal Teknologi dan Sistem Komputer, 4(3), 2016, 450-453

Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android

Widi Puji Atmojo[*)], R. Rizal Isnanto, Rinta Kridalukmana
Program Studi Sistem Komputer, Fakultas Teknik, Universitas Diponegoro
Jl. Prof. Soedarto, SH, Kampus Undip Tembalang, Semarang, Indonesia 50275

Abstract - Security is a very important aspect in data communication. In the last decade, there was a rapid development in mobile phone technology. Smartphone have been equipped with various features and one of them is the short message service (SMS). However, messages sent via mobile phone networks pose threat to be accessed by people who do not have any authorization. Therefore, it is necessary to do research on the development of software to enhance the security of messages through message encryption and decryption features. This application uses Java programming language with SDK (Software Development Kit) Android and Android Studio 1.3.1 as an editor. The initial step of this research is to encrypt the original message to produce the ciphertext message. The second step is to decrypt ciphertext incoming messages to become genuine message. Results from this research are an Android-based application that can perform encryption and decryption of the SMS messages using the RC6 algorithm. With the application of cryptography for SMS messages, the expected level of information security of the message can be improved so that the message will be more secure from unauthorized access.

Keywords – Android; SMS; Encryption; Decryption; RC6

I. PENDAHULUAN

Perkembangan teknologi, semakin maju berdampak pada cara masyarakat dalam berkomunikasi. Dahulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti *email*, SMS (*Short Messaging Service*), dan Internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan.

*) Penulis korespondensi
Email: widipujiatmojo@gmail.com

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh masyarakat luas, dan bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi dengan baik. Selain itu, pengiriman SMS yang dilakukan tidak sampai ke penerima secara langsung, namun pengiriman SMS harus melewati *Short Message Service Center* (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Dengan tersimpannya SMS pada SMSC, seorang operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut [9].

Dengan demikian dibutuhkan suatu metode dan aplikasi yang dapat memberikan solusi *encrypted end to end* dengan melakukan enkripsi terhadap pesan SMS. Enkripsi adalah proses mengubah suatu pesan asli yang disebut *plaintext* menjadi sebuah sandi atau kode yang tidak terbaca yang disebut *ciphertext* yang tidak dapat dimengerti.

Pada perkembangan teknologi saat ini, telepon selular berbasis Android telah banyak dipakai oleh banyak pengguna telepon selular. Selain itu, Android bersifat terbuka, gratis, dan hampir setiap kode program Android diluncurkan berdasarkan lisensi *open source* Apache yang berarti bahwa setiap orang yang ingin menggunakan Android dapat mengunduh penuh *source code* nya[10].

Sekarang ini terdapat berbagai algoritma kunci simetris yang dapat digunakan dalam penyandian data. Salah satunya adalah algoritma RC6 yang terkenal dengan algoritma yang sederhana namun memiliki tingkat keamanan yang tinggi. Algoritma RC6 membagi blok 128 bit menjadi 4 buah blok 32 bit, yaitu register A, B, C, D. Pada algoritma RC6, proses enkripsi dimulai dan diakhiri dengan proses *whitening* yang bertujuan untuk menyamarkan iterasi yang pertama dan yang terakhir dari proses enkripsi dan dekripsi. Selain itu, terdapat sub kunci yang dibentuk dari kombinasi kunci yang dimasukkan pengguna dengan kunci inisialisasi yang terdapat dalam algoritma RC6.

Perangkat lunak yang dibangun merupakan perangkat lunak yang diterapkan pada telepon selular yang bersistem operasi Android dan memiliki fungsi untuk melakukan enkripsi dan dekripsi pesan. Pesan

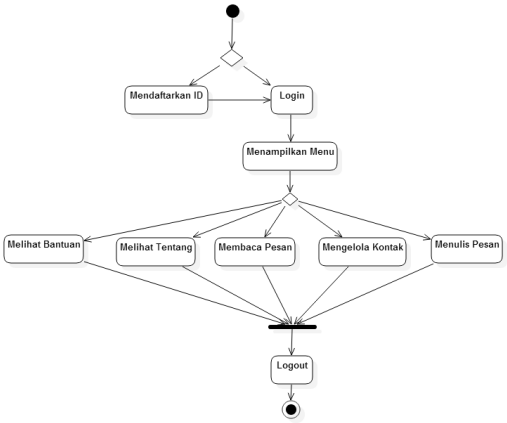
Dikirim:24 Juli 2016; Direvisi:6 Agustus 2016; Diterima:10 Agustus 2016

yang telah dibuat dikirimkan ke telepon selular lain melalui jaringan telepon selular.

II. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini menggunakan tahapan model *waterfall*. Menurut Pressman, Model *waterfall* merupakan pendekatan yang sistematis dan berurutan pada pengembangan perangkat lunak. Pengembangan dimulai dengan menentukan spesifikasi kebutuhan dan berlanjut melalui tahapan berikutnya. Menutut R. Tantra, tahapan yang secara umum dilalui adalah analisis kebutuhan (*requirement*) perangkat lunak, perancangan (*design*) sistem, implementasi perangkat lunak, pengujian (*verification*) dan pemeliharaan (*maintenance*) sistem.

Berikut diagram aktivitas sistem dari aplikasi yang dibangun ditunjukkan pada Gambar 1.

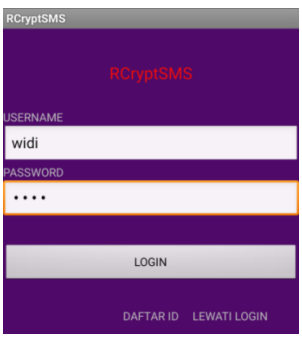


Gambar 1 Diagram Aktivitas Sistem

III. HASIL DAN PEMBAHASAN

1. Pengujian Login

Pengujian login dilakukan dengan memasukkan *username* dan *password* bagi pengguna yang telah melakukan registrasi akun seperti pada Gambar 2. Gambar 3 menunjukkan tampilan menu utama setelah pengguna berhasil login ke dalam sistem aplikasi.

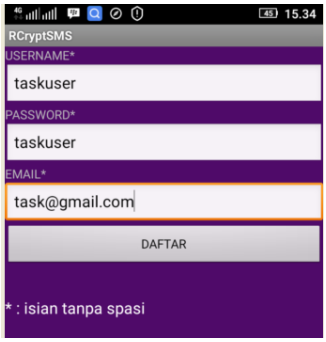


Gambar2 Pengujian pengguna saat mengisi form *login*

Gambar 3 Hasil pengujian *login* pengguna

1. Mendaftarkan ID

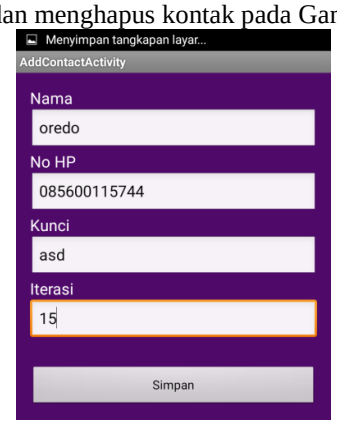
Pada pengujian ini terdapat proses pendaftaran data pengguna agar dapat melakukan fungsi *login* aplikasi. Data yang dapat diisikan yaitu *username*, *password*, dan alamat email pengguna. Gambar 4 ditampilkan antarmuka pengisian registrasi data pengguna.



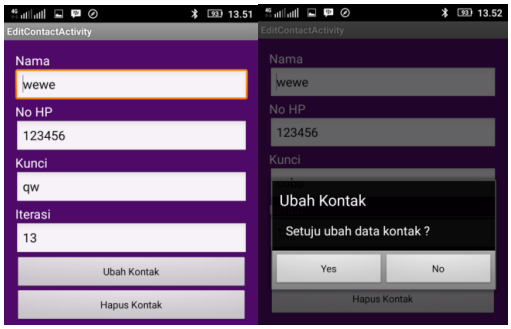
Gambar 4 Pengujian pengisian registrasi data pengguna

2. Pengujian Manajemen Kontak

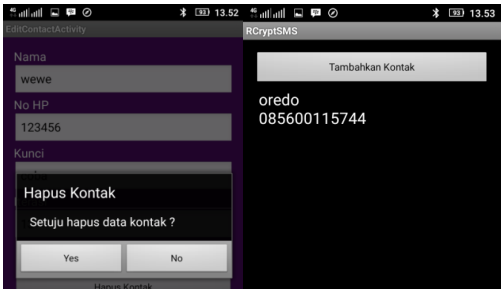
Dalam pengujian ini terdapat beberapa unit pengujian, diantaranya pengujian menambah kontak pada Gambar 5, pengujian mengubah kontak pada Gambar 6, dan menghapus kontak pada Gambar 7.



Gambar 5 Pengujian menambah kontak



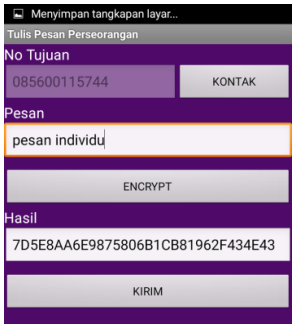
Gambar 6 Pengujian mengubah kontak



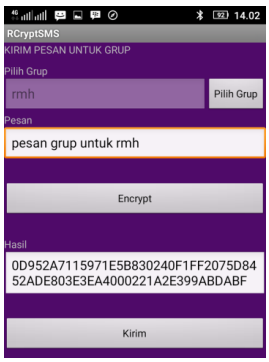
Gambar 7 Pengujian menghapus kontak

3. Pengujian Menulis Pesan

Pengujian ini adalah aktivitas yang dapat dilakukan pengguna untuk mengirimkan pesan SMS ke satu pihak penerima pesan (ditunjukkan pada Gambar 8) dan ke anggota grup (ditunjukkan pada Gambar 9) dalam bentuk *ciphertext* setelah melakukan proses enkripsi. Pesan dapat dikirim ke penerima pesan setelah pengguna menekan tombol **Kirim.**



Gambar 8 Pengujian tulis pesan perorangan

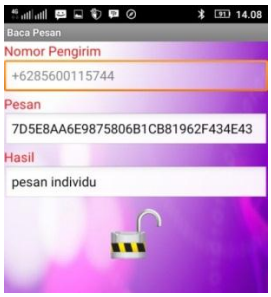


Gambar 9 Pengujian tulis pesan grup

4. Pengujian Membaca Pesan

Pengujian ini adalah aksi yang dapat dilakukan pengguna untuk mengubah pesan *ciphertext* ke dalam bentuk pesan asli. Gambar 10 menunjukkan pengujian memilih pesan dan Gambar 11 menunjukkan pengujian membaca pesan.

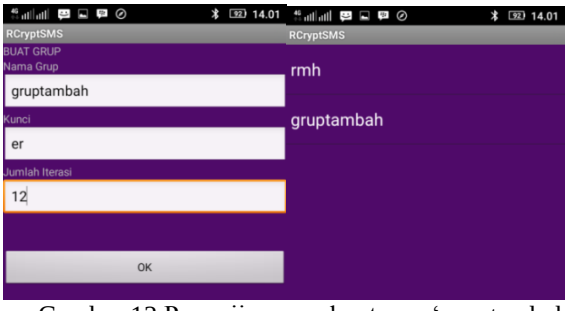
Gambar 10 Pengujian memilih pesan



Gambar 11 Pengujian membaca pesan

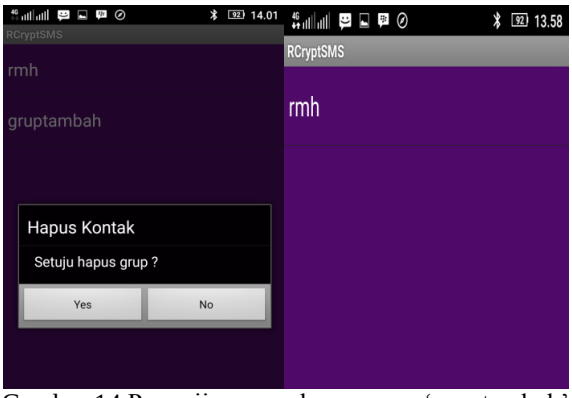
5. Pengujian Manajemen Grup dan Anggota

Dalam pengujian ini terdapat beberapa unit pengujian, diantaranya pengujian membuat grup pada Gambar 12, pengujian mengubah grup pada Gambar 13, pengujian menghapus grup pada Gambar 14, dan pengujian menambah anggota pada Gambar 15, pengujian menghapus anggota grup pada Gambar 16.

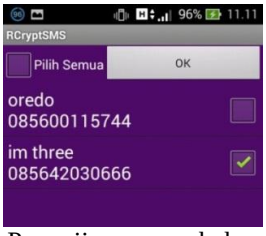


Gambar 12 Pengujian membuat grup‘gruptambah’

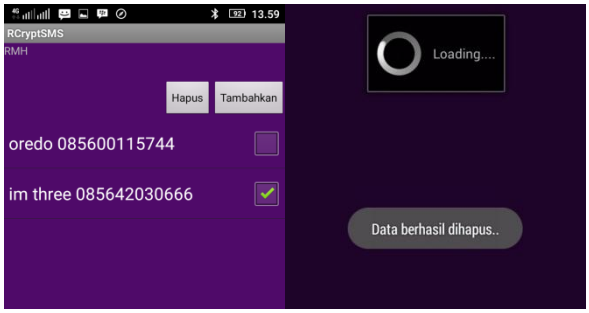
Gambar 13 Pengujian mengubah grup ‘gruptambah’



Gambar 14 Pengujian menghapus grup ‘gruptambah’



Gambar 15 Pengujian menambah anggota grup



Gambar 16 Pengujian menghapus anggota grup ‘rmh’

IV. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan, dapat disimpulkan beberapa hal, diantaranya aplikasi penyandi SMS ini dapat menyandikan pesan asli (*plaintext*) menjadi pesan tersandi (*ciphertext*) dalam format heksadesimal melalui proses enkripsi pesan SMS. Begitu juga pada proses dekripsi pesan dapat dilakukan untuk mengubah pesan *ciphertext* menjadi pesan asli agar dapat dimengerti oleh penerima pesan SMS. Kedua, bila jumlah iterasi yang dimasukkan pengguna (iterasi digunakan untuk melakukan rotasi algoritma RC6) semakin besar, maka tingkat keamanan akan semakin baik, tetapi waktu yang dibutuhkan akan semakin besar untuk melakukan proses enkripsi maupun dekripsi pesan. Ketiga, *ciphertext* (pesan tersandi) yang merupakan hasil proses enkripsi dalam aplikasi dapat dikirimkan ke penerima pesan SMS melalui jaringan telepon selular. Aplikasi dapat berlajan dengan baik dalam mengakses basis data untuk menyimpan data kontak penerima dan data grup sms. Yang terakhir, nomor telepon selular penerima pesan harus terlihat pada pengaturan telepon untuk dapat mendekripsi pesan *ciphertext*.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada seluruh civitas akademik Prodi Sistem Komputer Undip yang telah memberikan berbagai masukan terhadap penelitian yang sudah dilaksanakan, serta pemberian berbagai ilmu yang sangat bermanfaat. Dan juga tersedianya fasilitas laboratorium yang telah memberikan fasilitas pengujian dan penunjang kegiatan akademik.

DAFTAR PUSTAKA

[1] Abdurohman, M. (2002). Analisis Performansi Algoritma Kriptografi RC6. Journal Departemen Teknik Elektro ITB.

[2] Ariyus, D. (2006). *Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

[3] Ariyus, D. (2008). *Pengantar Ilmu KRIPTOGRAFI*. Yogyakarta: Graha Ilmu.

[4] Defni, I.R. (2014). Enkripsi SMS (Short Message Service) pada Telepon Seluler Berbasis Android Dengan Metode RC6. *J. Momentum* 16, 63–73.

[5] Muharini, A. (2012). Universitas Indonesia. *Aplikasi Algoritma Rivest Code 6 dalam Pengamanan Citra Digital*.

[6] Permana, R.W.A. (2008). Institut Teknologi Bandung. *Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular*.

[7] R. Pressman. (2012). *Rekayasa Perangkat Lunak*. Yogyakarta: ANDI.

[8] R. Tantra. (2012). *Manajemen Proyek Sistem Informasi*. Yogyakarta: ANDI.

[9] Safaat, N. (2015). *Aplikasi Berbasis Android*. Bandung: Informatika.

[10] Safaat, N. (2012). *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Bandung: Informatika.