VOL. 17 NO. 3 SEPTEMBER 2016

ISSN : 1411-3201

Jurnal Ilmiah DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

STMIK AMIKOM
YOGYAKARTA

VOL. 17 NO. 3 SEPTEMBER 2016 ISSN:1411-3201

JURNAL ILMIAH DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

STMIK AMIKOM
YOGYAKARTA

VOL. 17 NO. 3 SEPTEMBER 2016
JURNAL ILMIAH
Data Manajemen Dan Teknologi Informasi

Terbit empat kali setahun pada bulan Maret, Juni, September dan Desember berisi artikel hasil penelitian dan kajian analitis kritis di dalam bidang manajemen informatika dan teknologi informatika. ISSN 1411-3201, diterbitkan pertama kali pada tahun 2000.

PENANGGUNG JAWAB :
Ketua STMIK AMIKOM Yogyakarta, Prof. Dr. M. Suyanto, M.M.

ALAMAT PENYUNTING & TATA USAHA
STMIK AMIKOM Yogyakarta, Jl. Ring Road Utara Condong Catur Yogyakarta, Telp. (0274) 884201 Fax. (0274) 884208, Email : jurnal@amikom.ac.id

BERLANGGANAN
Langganan dapat dilakukan dengan pemesanan untuk minimal 4 edisi (1 tahun)
pulau jawa Rp. 50.000 x 4 = Rp. 200.000,00 untuk luar jawa ditambah ongkos kirim.

VOL. 17 NO. 3 SEPTEMBER 2016 **ISSN : 1411- 3201**

JURNAL ILMIAH

DASI

DATA MANAJEMEN DAN TEKNOLOGI INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

JURNAL ILMIAH

DASI

KATA PENGANTAR

Puji syukur kehadlirat Tuhan Yang Maha Kuasa atas anugerahnya sehingga jurnal edisi kali ini berhasil disusun dan terbit. Beberapa tulisan yang telah melalui koreksi materi dari mitra bestari dan revisi redaksional dari penulis, pada edisi ini diterbitkan. Adapun jenis tulisan pada jurnal ini adalah hasil dari penelitian dan pemikiran konseptual. Redaksi mencoba selalu mengadakan pembenahan kualitas dari jurnal dalam beberapa aspek.

Beberapa pakar di bidangnya juga telah diajak untuk berkolaborasi mengawal penerbitan jurnal ini. Materi tulisan pada jurnal berasal dari dosen tetap dan tidak tetap STMIK AMIKOM Yogyakarta serta dari luar STMIK AMIKOM Yogyakarta.

Tak ada gading yang tak retak begitu pula kata pepatah yang selalu di kutip redaksi, kritik dan saran mohon di alamatkan ke kami baik melalui email, faksimile maupun disampaikan langsung ke redaksi. Atas kritik dan saran membangun yang pembaca berikan kami menghaturkan banyak terimakasih.

Redaksi

DAFTAR ISI

PERANCANGAN PESAN RAHASIA APLIKASI SMS MENGGUNAKAN ALGORITMA RC6 BERBASIS ANDROID (Studi Kasus: PT. Time Excelindo)

Jefrul Hanafi [1)] **, Hartatik** [2)]

[1)] *Teknik Informatika STMIK AMIKOM Yogyakarta*
[2)] *Manajemen Informatika STMIK AMIKOM Yogyakarta*
email : jefrul.h@students.amikom.ac.id[1)], *hartatik@amikom.ac.id*[2)]

Abstraksi

SMS (*Short Message Service*) adalah pesan singkat yang sangat banyak digunakan oleh masyarakat . tidak semua orang tahu bahwa keamanan jaringan di SMS (*Short Message Service*) sangat rendah . SMS merupakan media komunikasi yang tidak titik - to - point , belum tentu pesan yang dikirim langsung ke tujuan . data penting yang kirim via SMS mudah dibaca dan dicegat. Salah satu solusi untuk mengatasi masalah ini adalah dengan menggunakan algoritma kriptografi dalam aplikasi perangkat lunak atau SMS. Algoritma RC6 adalah algoritma dengan parameter kunci pribadi yang dapat bekerja pada beragam kunci. Algoritma RC6 Enkripsi sangat terkenal sekali dengan kesederhanaan yang dapat melakukan enkripsi dan dekripsi. Hasil penelitian ini menunjukkan bahwa aplikasi SMS pada smartphone yang tertanam dengan algoritma Rivest Code (RC6) dapat melindungi informasi penting dengan benar.

***Kata Kunci* :**
Kriptografi, RC6, Enkripsi, Dekripsi, SMS.

Abstract

SMS (Short Message Service) is a short message that is very much used by the public. not everyone knows that the network security in SMS (Short Message Service) is very low. SMS is a medium of communication that is not a point - to - point, not necessarily a message sent directly to the destination. the important data which is send via SMS easy to read and intercepted. One of the solution to handle this problem is using a cryptographic algorithm in an application software or SMS. RC6 algorithm is an algorithm with a private key parameters that can work on diverse key. RC6 Encryption algorithm is very well known at all by the simplicity that can perform encryption and decryption. Result of this research show that SMS application on a smartphone that embedded with of algorithms Rivest Code (RC6) may protect critical information properly.

***Keywords* :**
Kriptografi, RC6, Enkripsi, Dekripsi, SMS.

Pendahuluan

Kemajuan dan perkembangan teknologi telekomunikasi yang begitu pesat dan besar manfaatnya terhadap kebutuhan masyarakat luas. Salah satunya yang menjadi kebutuhan utama masyarakat yaitu keamanan pada data. Keamanan pada data merupakan aspek terpenting dari sebuah sistem informasi.

Pada dasarnya manusia tidak lepas dari hal yang disebut komunikasi. Salah satunya pada telepon selululer yang berupa pesan singkat atau SMS (*Short Message Service*). Telepon seluler dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka (di udara) yang sangat rentan akan ancaman seperti penyadapan oleh pihak yang tidak bertanggung jawab. Sebab, SMS merupakan media komunikasi yang bukan point-to-point, tentu pesan yang dikirimkan tidak langsung sampai pada tujuan.

Oleh karena itu penulis mencoba merancang sebuah aplikasi SMS sederhana dengan penerapan algoritma kriptografi RC6 pada android yang memberikan keamanan dengan enkripsi pada sebuah teks berupa pesan singkat atau SMS. Dan bisa dibaca oleh penerima pesan dengan menggunakan aplikasi dan kunci yang sama untuk membaca pesan tersebut dengan kata lain yaitu dekripsi pada pesan rahasia yang telah dienkripsi oleh pengirim.

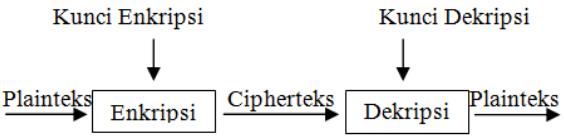
Tinjauan Pustaka

Defini dan Indri Rhamayun dosen jurusan Teknologi Informasi Politeknik Negeri Padang dalam jurnalnya yang berjudul "ENKRIPSI SMS (SHORT MESSAGE) PADA TELEPON SELULAR BERBASIS ANDROID DENGAN METODE RC6". Hasil dari penelitian ini diimplementasikan pada smartphone berbasis android yang berjalan pada sistem operasi minimal android 2.2 (froyo) ke atas yang mempunyai API (*Application Programing Interface*) minimum level 8. [1]

Muhammad Indra dari STMIK Amikom Yogyakarta pada skripsinya yang berjudul "Implementasi Algoritma RC6 Untuk Enkripsi Dan Dekripsi SMS Berbasis Android". Tujuan dari skripsinya adalah menerapkan algoritma RC6 untuk aplikasi enkripsi atau dekripsi pesan sebagai upaya mengamankan suatu informasi pada layanan pesan singkat (SMS). Dari hasil penelitiannya ini dapat diterapkan pada aplikasi berbasis android yang berjalan pada system operasi minimal android 2.2 (froyo) ke atas [2].

Pengertian Kriptografi

Kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi dua kripto dan graphia, kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan dikirim dari suatu tempat ketempat yang lain. [3]



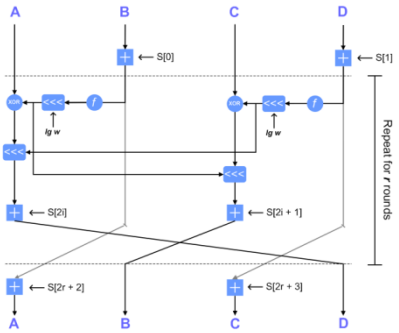
Gambar 1. Sistem Kriptografi

Algoritma RC6

RC6 merupakan salah satu algoritma kriptografi kunci simetris yang berbentuk block chipper salah satu kandidat dalam penentuan algoritma standar untuk kriptografi DES yang sekarang disebut AES. Algoritma ini merupakan pengembangan dari algoritma sebelumnya yang dikembangkan dari RC5 oleh Ronald Linn Rivest, Ray Sidney, Matt JB.Robshaw dan Yiquin Yin dari RSA security, Inc. Pada tahun 1998.Dan telah memenuhi kriteria yang diajukan oleh NIST (National Institute of Standards and Technology).

Enkripsi

Fungsi enkripsi menerima input 1 blok *plaintext* yang terdapat dalam 4 register yang masing-masing berupa w-*bit word*, yaitu A, B, C, dan D. *Ciphertext* hasil proses terbagi dan disimpan dalam A, B, C, dan D. Dalam proses enkripsi diperlukan tabel kunci S yang dianggap telah didapat dari proses sebelumnya.

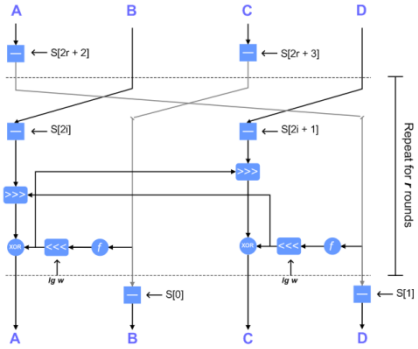


Gambar 2. Diagram Enkripsi RC6

dengan $f(x) = x*(2x + 1)$

Dekripsi

Proses dekripsi *ciphertext* pada algoritma RC6 merupakan pembalikan dari proses enkripsi. Pada proses *whitening*, bila proses enkripsi menggunakan operasi penjumlahan, maka pada proses dekripsi menggunakan operasi pengurangan.



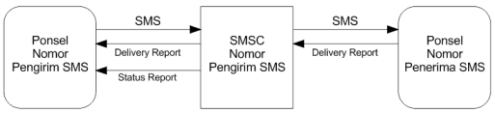
Gambar 3. Diagram Dekripsi RC6 dengan $f(x) = x*(2x + 1)$

UML (*Unified Modeling Language*)

Unified Modeling Language (UML) adalah keluarga notasi grafis yang didukung oleh meta-model tunggal, yang membantu pendeskripsian dan desain sistem perangkat lunak, khususnya sistem yang dibangun menggunakan pemrograman berorientasi objek (OO). [5]

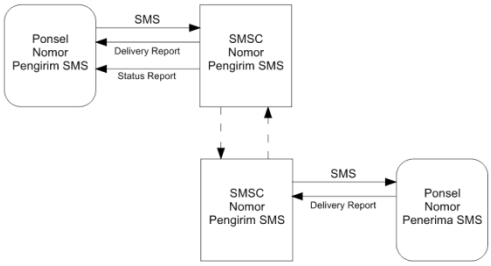
Pengertian SMS (*Short Message Service*)

SMS merupakan suatu sistem pengiriman pesan sederhana yang disediakan oleh jaringan telepon seluler. Fitur SMS ini didukung oleh GSM (*Global System for Mobile Communication*), TDMA (*Time Multiple Digital Access*), CDMA (*Code Multiple Digital Access*). [4]



Gambar 4. Mekanisme *Intra-Operator* (satu operator)

SMS yang dikirmkan oleh nomor pengirim akan dimasukkan terlebih dahulu ke dalam SMSC operator nomor pengirim, kemudian SMSC tersebut akan mengirimkan ke nomor yang dituju secara langsung. Nomor penerima kemudia akan mengirimkan sebuah *deliveryreport* yang menyatakan bahwa SMS telah diterima SMSC. SMSC kemudian meneruskan *report* tersebut ke nomor pengirim SMS, disertai *status report* dari proses pengiriman SMS tersebut.



Gambar 5. Mekanisme *Inter-Operator* (dua operator)

Dari gambar diatas, selain masuk ke SMSC operator pengirim, SMS yang dikirimkan akan diteruskan oleh SMSC operator pengirim ke SMSC operator penerima SMS, kemudian baru diteruskan ke nomor tujuan, *delivery report*yang dihasilkanpun harus melewati mekanisme yang sama sebelum diterima oleh nomor pengirim.

Metode Penelitian

Penelitian ini dilakukan melalui beberapa tahapan sebagai berikut :

1. Pengumpulan data
   Pengumpulan data dilakukan melalui beberapa tahapan seperti wawancara, studi litartur dan pengumpulan data sekunder melalui internet dan blog.
2. Analisis sistem
   Analisis sistem dilakukan dengan menggunakan analisis SWOT guna mencari kekuatan, kelemahan dan peluang dari sistem yang ada sekarang ini.
3. Perancangan Sistem
   Perancangan sistem dibuat dengan menggunakan diagram UML guna menemukan fitur dan aliran data yang akan dibuat di sistem
4. Pengkodingan
5. Pengujian
   Pengujian dilakukan menggunakan metode *Black Box Testing* guna menguji fungsionalitas fitur yang sudah dibuat.

Hasil dan Pembahasan

Analisis Sistem

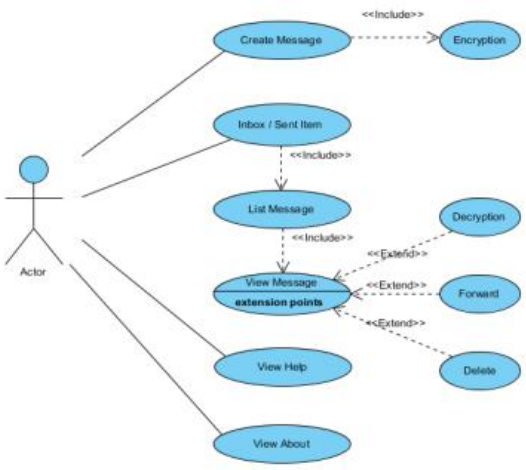
Analisis sistem dilakukan untuk mengetahui bagaimana memahami dan menjelaskan secara rinci tentang kebutuhan sistem dalam mengembangkan sebuah aplikasi.

Tabel 1. Analisis SWOT

Internal / Eksternal	Strength	Weakness
	1. Memberikan keuntungan berupa keamanan. 2. Memberikan kemudahan yang efektif dan efisen bagi pengguna dalam melakukan enkripsi dekripsi pada pesan SMS. 3. Memiliki kemampuan untuk beroperasi pada mode blok 128 bit. 4. Proses enkripsi tidak tergantung pada panjang kunci maupun panjang pesan. Sehingga, waktu yang dibutuhkan untuk membangun sebuah kunci adalah sama, walupun kuncinya adalah 128, 192, atau 256 bit. Begitu juga untuk panjangnya karakter pada pesan.	1. Aplikasi ini hanya dapat mengirimkan pesan ke satu nomor dalam satu waktu. 2. Aplikasi ini berjalan pada sistem operasi android, sehingga pengirim dan penerima pesan harus menggunakan ponsel berbasis android dengan batas minimum 2.2 (*froyo*). 3. Untuk enkripsi pesan ialah membuat pesan yang akan dikirimkan menjadi lebih panjang dari pesan aslinya. 4. Prose pengiriman hanya menggunakan 1 SIM yaitu SIM Default.
Opportunity	**WO**	**SO**
1. Dari informasi akhir tahun 2015 menyatakan bahwa pengguna smartphone berbasis android begitu besar di Indonesia mencapai 55 juta pengguna. Ini memberikan peluang dalam penggunaan aplikasi berbasis android. 2. Sistem Operasi android yang bersifat *open source* (gratis) memberikan kemudahan bagi *Developer* Android.	1. Merancang tampilan yang nyaman dan mudah digunakan. 2. Menambahkan algoritma enkripsi agar jenis pengenkripsian dan tingkat keamanannya lebih bervariasi.	1. Penambahan sistem broadcast pada aplikasi SMS sehingga dapat mengirimkan pesan ke beberapa nomor dalam sekali pengiriman. 2. Mengembangkan aplikasi dalam beberapa platform agar pemasaran semakin luas.
Threats	**WT**	**ST**
1. Adanya kriptanalis yang hendak mencoba memecahkan algoritma kriptografi dengan berbagai macam serangan	1. Mengembangkan aplikasi dalam beberapa platform agar aplikasi enkripsi masih tetap bisa dipelajari lebih dalam dan dikembangkan guna meningkatkan	1. Memanfaatkan respon dari *user*, guna meminimalisir kekurangan dari aplikasi. 2. Mengantisipasi ancaman dari luar seperti serangan diferensial dan

seperti diferensial dan linear. 2. Tidak menutup kemungkinan bahwa akan selalu banyak yang menggunakan smartphone berbasis android.	keamanan pada data yang di sandikan (enkripsi). 2. Menginputkan panjang bit kunci yang lebih panjang pada saat enkripsi pesan.	linear dengan menganalisa jenis-jenis serangan dengan menggunakan aplikasi-aplikasi tertentu dan juga jurnal-jurnal sebagai referensi. 3. Membangun operasi primitf-primtif yang lebih baik supaya terhindar dari serangan linear. 4. Menerapkan fitur *data-dependent rotations* secara lebih baik agar terhindar dari serangan diferensial dan linear.

Perancangan *Use Case*

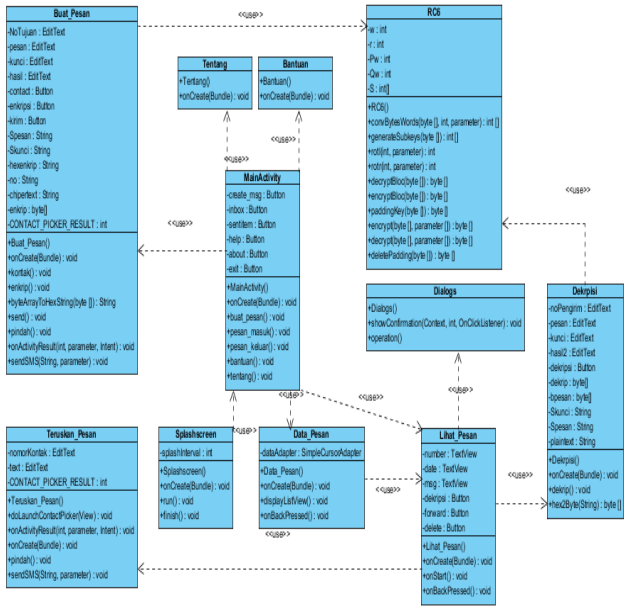


Gambar 6. Use Case Diagram

Fungsi Case dari dari gambar 6 adalah :

1. *Use Case Create Message*
   Use Case yang menggambarkan proses buat pesan yang terjadi pada *Use Case Encryption* bertujuan untuk menyandikan pesan sebelum dikirim oleh aktor atau pengguna dengan memasukkan kunci pada *form key*.
2. *Use Case Inbox / Sent Item*
   Use Case yang didalamnya terdapat beberapa use case yang akan diproses yaitu *Use Case List* pesan, dan *Use Case* Lihat Pesan. *Use Case* Lihat Pesan ini akan memproses beberapa use case lagi yaitu *Use Case Decryption, Use Case Forward,* dan *Use Case Delete.* Dimana tujuan dari *Use Case Inbox / Sent Item* ini adalah untuk melihat pesan masuk atau keluar baik itu pesan yang terenkripsi dengan cara menjalankan fungsi dari *Use Case Decryption* dengan cara memasukkan sandi yang sama dalam proses enkripsi, begitu juga dengan pesan biasa yang tidak terenkripsi.
3. *Use Case Help*
   Use Case yang menampilkan sebuah halaman bantuan bagi pengguna yang kurang paham akan penggunaan aplikasi tersebut.
4. *Use Case About*
   Use Case yang menampilkan halaman informasi umum aplikasi bagi pengguna.

Perancangan *Class Diagram*



Gambar 7. *Class Diagram*

Class Diagram

Class MainActivity merupakan *class* inti yang akan berhubungan dengan *class-class* lainnya. *Class* ini akan muncul setelah *class SplashScreen* diproses. Apabila pengguna hendak melakukan enkripsi sebuah pesan, maka *class* ini akan memanggil *class* Buat_Pesan sebagai halaman interaksi pengguna dengan sistem sehingga inputan yang dimasukkan pengguna akan diproses oleh *class RC6* sebagai *class* yang bertanggung jawab untuk enkripsi dan dekripsi secara detil dengan bahasa pemrograman java.

Dekripsi sebuah pesan dapat dilakukan apabila pesan tersebut telah terenkripsi menggunakan kunci yang sama. Sehingga nanti *class* Dekripsi ini akan berhubungan dengan *class RC6* sebagaimana *class* Buat_Pesan.

Pesan masuk atau keluar akan diambil oleh class lihat pesan dari class data_pesan yang akan ditampilkan pada pengguna dalam bentuk pesan lengkap, yang nantinya bisa diteruskan dengan memanggil *class* Teruskan_Pesan begitu juga dengan penghapusan ataupun pembacaan pesan yang

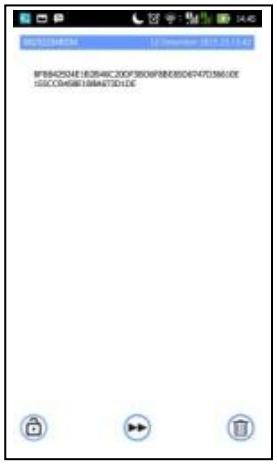
terenkripsi. Sedangkan *class Inbox / Sent Item* hanya menampilkan daftar pesan.

Interface

Interface dari aplikasi yang dibuat dapat dilihat pada gambar 8 sampai dengan gambar 16.

Gambar 8. *Splas Screen*, Gambar 9.Menu Utama

Gambar 10. Daftar Pesan, Gambar 11. Enkripsi



Gambar 12. Lihat Pesan, Gambar 13. Dekrpisi

Gambar 14. Teruskan **Gambar 15. Bantuan**

Pengujian dengan *Black-Box Testing*

Pengujian dengan Black-box Testing ini dilakukan pada seluruh modul program untuk mengetahui apakah program yang dibuat sudah sesuai dengan kebutuhan fungsionalnya. Berikut beberapa kategori yang akan diuji menggunakan *Black-box Testing*:

1. Fungsi-fungsi yang tidak benar atau hilang
3. Kesalahan kinerja sistem
4. Kesalahan tampilan (*interface*)

Tabel 2. *Testing* Masuk Aplikasi

No	Skenario	Hasil	Status
1	Tekan *icon* aplikasi pada *device*	Tampil *splash screen* selama 3 detik, masuk menu utama	Berhasil

Tabel 3. *Testing* Masuk Aplikasi

No	Skenario	Hasil	Status
1	Tekan tombol *create*	Masuk ke halaman buat pesan	Berhasil
2	Tekan tombol *inbox*	Masuk ke halaman daftar pesan masuk	Berhasil
3	Tekan tombol *sent item*	Masuk ke halaman daftar pesan terkirim	Berhasil
4	Tekan tombol *help*	Masuk ke halaman bantuan	Berhasil
5	Tekan tombol *about*	Masuk ke halaman tentang	Berhasil
6	Tekan tombol *exit*	Keluar dari aplikasi	Berhasil

Tabel 4. *Testing* Buat Pesan (*encryption*)

No	Skenario	Hasil	Status
1	Tekan tombol *contact*	Tampil daftar kontak	Berhasil
2	Tekan tombol *encryption*	Pesan akan di enkripsi dan berubah menjadi *ciphertext* berupa bilangan heksadesimal apabila pengguna telah menginputkan kunci pada kolom *key* dan pesan pada kolom *message*.	Berhasil
3	Tekan tombol *send*	Pesan akan dikirmkan ke nomor tujuan, jika pesan berhasil terkirim maka akan kembali	Berhasil

		ke halaman menu utama	

Tabel 5. *Testing* Daftar Pesan

No	Skenario	Hasil	Status
1	*Scroll* untuk memilih pesan	Daftar pesan dapat di-*scroll* ke arah atas dan bawah	Berhasil
2	Tekan pesan yang dipilih	Menampilkan pesan secara utuh pada halaman lihat pesan	Berhasil

Tabel 6. *Testing* Baca Pesan (*decryption*)

No	Skenario	Hasil	Status
1	Pilih tombol *decryption* pada halaman lihat pesan	Masuk ke halaman baca pesan (*decryption*)	Berhasil
2	Tekan tombol *decryption*	Pesan akan dapat terbaca apabila pengguna menginputkan kunci yang benar pada kolom key	Berhasil

Tabel 7. *Testing* Teruskan Pesan (*forward*)

No	Skenario	Hasil	Status
1	Pilih tombol teruskan pesan pada halaman lihat pesan	Masuk ke halaman teruskan pesan	Berhasil
2	Tekan tombol *contact*	Menampilkan daftar kontak, pilih kontak maka akan tampil kontak yang dipilih pada kolom kontak	Berhasil
3	Tekan tombol *send*	Pesan akan diteruskan jika pengguna telah menginputkan kontak dan kembali kehalaman menu utama.	Berhasil

Tabel 8. *Testing* Hapus Pesan (*delete*)

No	Skenario	Hasil	Status
1	Pilih tombol *delete* pada halaman lihat pesan	Muncul dialog "Apakah Anda Yakin Akan Menghapus SMS Ini?", pengguna memilih Ya atau Tidak	Berhasil
2	Pilih Ya	Pesan yang dipilih akan terhapus dan kembali ke halaman daftar pesan	Berhasil

Tabel 9. *Testing* Tentang

No	Skenario	Hasil	Status
1	Tekan tombol *about*	Masuk ke halaman tentang	Berhasil

Tabel 10. *Testing* Tentang

No	Skenario	Hasil	Status
1	Tekan tombol *help*	Masuk ke halaman bantuan	Berhasil

Kesimpulan dan Saran

Kesimpulan dari penelitian ini adalah

1. Aplikasi SMS pada smartphone yang tertanam dengan algoritma Rivest Code (RC6) dapat melindungi informasi penting dengan benar.
2. Belum adanya mekanisme pendistribusian kunci yang aman membuat user kesulitan dalam pengaturan kunci.

Daftar Pustaka

[1] Indri. Defnidan, 2014, *Enkripsi SMS (Short Message Service) Pada Selular Berbasis Android Dengan Metode RC6*, http://ejournal.itp.ac.id/index.php/momentum/article/download/160/159, diakses pada28 Januari 2016.

[2] Indra, Muhammad., *Implementasi Algoritma RC6 Untuk Enkripsi Dan Dekripsi SMS Berbasis Android*, Yogyakarta: Skripsi STMIK Amikom, 2014.

[3] Ariyus, Doni., 2006, *Kriptografi*, Keamanan Data, dan Komunikasi. GRAHA ILMU.

[4] Riadi, Muchlisin, 2012, *Teori SMS (Short Message Service)*, www.kajianpustaka.com/2012/12/teori-sms-short-message-service.html, diakses pada 20 Mei 2016.

[5] Fowler, Martin., 2005, *UML Distilled Panduan Singkat Bahasa Pemodelan Objek Standar*. ANDI OFFSET.