

INFORMASI INTERAKTIF

JURNAL INFORMATIKA DAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK INFORMATIKA – FAKULTAS TEKNIK -UNIVERSITAS JANABADRA

MODIFIKASI KRIPTOGRAFI KLASIK VIGENERE CIPHER MENGGUNAKAN ONE TIME PAD DENGAN ENKRIPSI BERLANJUT

M. Ziaurrahman, Ema Utami, Ferry Wahyu Wibowo

PERBANDINGAN METODE WEIGHTED PRODUCT DAN SIMPLE ADDITIVE WEIGHTING DALAM SELEKSI PENGURUS FORUM ASISTEN (STUDI KASUS : UNIVERSITAS AMIKOM YOGYAKARTA)

Musthofa Galih Pradana, Kusri, Emha Taufiq Luthfi

APLIKASI SECURE-MESSAGE DENGAN ALGORITMA RC6 (RIVEST CODE 6) BERBASIS ANDROID

Arif Susanto Adhy, Fatsyahrina Fitriastuti, Jemmy Edwin Bororing

ANALISIS PERBANDINGAN SIMULASI LOAD BALANCE MENGGUNAKAN METODE ECMC DAN PCC PADA PENERAPAN KONGESTI MANAJEMEN BANDWIDTH HTB (STUDI KASUS: UNIVERSITAS KRISTEN IMMANUEL, YOGYAKARTA)

Azriel Christian Nurcahyo, Ema Utami, Suwanto Raharjo

EVALUASI INVESTASI TEKNOLOGI INFORMASI DENGAN MENGGUNAKAN DOMAIN VALUE GOVERNANCE VAL IT FRAMEWORK 2.0 (STUDI KASUS: CV.BERKA)

Ferdy Firmansyah, Wing Wahyu Winarno, Asro Nasiri

PREDIKSI PENJUALAN KOSMETIK DENGAN SUPPORT VECTOR MACHINE

Aflahah Apriliyani, Ema Utami, Suwanto Raharjo

ANALISIS PENERIMAAN APLIKASI GABLIND MENGGUNAKAN METODE UNIFIED THEORY OF ACCEPTANCE AND USE OF TECHNOLOGY TERHADAP PERILAKU PENGGUNA

Monalisa Fatmawati Sarifah, Ema Utami, Asro Nasiri

PERANCANGAN SISTEM PAKAR FINAL CHECK MOTOR MATIC MENGGUNAKAN METODE FORWARD CHAINING STUDI KASUS AHASS 9677

Wahit Desta Prastowo, Kusri, Ferry Wahyu Wibowo

KLASIFIKASI AUDIO MENGGUNAKAN WAVELET TRANSFORM DAN NEURAL NETWORK

Yulianto Mustaqim, Ema Utami, Suwanto Raharjo



DEWAN EDITORIAL

- Penerbit** : Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra
- Ketua Penyunting (Editor in Chief)** : Sofyan Lukmanfiandy, S.Kom., M.Kom. (Universitas Janabadra)
- Penyunting (Editor)** : 1. Eri Haryanto, S.Kom., M.Kom. (Universitas Janabadra)
2. Agustin Setiyorini, S.Kom., M.Kom. (Universitas Janabadra)
3. Sri Rahayu, S.Kom., M.Eng. (Universitas Janabadra)
4. Meilany Nonsi Tentua, S.Si., M.T. (Universitas PGRI Yogyakarta)
5. Agus Sasmito, S.Kom., M.Cs. *UPN Veteran Yogyakarta)
- Alamat Redaksi** : Program Studi Teknik Informatika Fakultas Teknik
Universitas Janabadra
Jl. Tentara Rakyat Mataram No. 55-57
Yogyakarta 55231
Telp./Fax : (0274) 543676
E-mail: informasi.interaktif@janabadra.ac.id
Website : <http://e-journal.janabadra.ac.id/>
- Frekuensi Terbit** : 3 kali setahun

JURNAL INFORMASI INTERAKTIF merupakan media komunikasi hasil penelitian, studi kasus, dan ulasan ilmiah bagi ilmuwan dan praktisi dibidang Teknik Informatika. Diterbitkan oleh Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra di Yogyakarta, tiga kali setahun pada bulan Januari, Mei dan September.

DAFTAR ISI

	<i>halaman</i>
Modifikasi Kriptografi Klasik <i>Vigenere Cipher</i> Menggunakan <i>One Time Pad</i> Dengan Enkripsi Berlanjut M. Ziaurrahman, Ema Utami, Ferry Wahyu Wibowo	63 - 68
Perbandingan Metode <i>Weighted Product</i> dan <i>Simple Additive Weighting</i> dalam Seleksi Pengurus Forum Asisten (Studi Kasus : Universitas Amikom Yogyakarta) Musthofa Galih Pradana, Kusrini, Emha Taufiq Luthfi	69 - 77
Aplikasi <i>Secure-Message</i> dengan Algoritma RC6 (<i>Rivest Code 6</i>) Berbasis Android Arif Susanto Adhy, Fatsyahrina Fitriastuti, Jemmy Edwin Bororing	78 - 83
Analisis Perbandingan Simulasi <i>Load Balance</i> Menggunakan Metode ECMC dan PCC pada Penerapan Kongesti Manajemen Bandwidth HTB (Studi Kasus: Universitas Kristen Immanuel, Yogyakarta) Azriel Christian Nurcahyo, Ema Utami, Suwanto Raharjo	84 - 93
Evaluasi Investasi Teknologi Informasi dengan Menggunakan Domain <i>Value Governance</i> Val IT Framework 2.0 (STUDI KASUS: CV.BERKA) Ferdy Firmansyah, Wing Wahyu Winarno, Asro Nasiri	94 - 100
Prediksi Penjualan Kosmetik dengan Support <i>Vector Machine</i> Aflahah Apriliyani, Ema Utami, Suwanto Raharjo	101 - 106
Analisis Penerimaan Aplikasi Gablind Menggunakan Metode <i>Unified Theory Of Acceptance and Use Of Technology</i> terhadap Perilaku Pengguna Monalisa Fatmawati Sarifah, Ema Utami, Asro Nasiri	107 - 113
Perancangan Sistem Pakar <i>Final Check Motor Matic</i> Menggunakan Metode <i>Forward Chaining</i> Studi Kasus Ahas 9677 Wahit Desta Prastowo, Kusrini, Ferry Wahyu Wibowo	114 - 121
Klasifikasi Audio Menggunakan <i>Wavelet Transform</i> dan Neural Network Yulianto Mustaqim, Ema Utami, Suwanto Raharjo	122 - 130

PENGANTAR REDAKSI

Puji syukur kami panjatkan kehadiran Allah Tuhan Yang Maha Kuasa atas terbitnya JURNAL INFORMASI INTERAKTIF Volume 4, Nomor 2, Edisi Mei 2019. Pada edisi kali ini memuat 9 (sembilan) tulisan hasil penelitian dalam bidang teknik informatika.

Harapan kami semoga naskah yang tersaji dalam JURNAL INFORMASI INTERAKTIF edisi Januari tahun 2019 dapat menambah pengetahuan dan wawasan di bidangnya masing-masing dan bagi penulis, jurnal ini diharapkan menjadi salah satu wadah untuk berbagi hasil-hasil penelitian yang telah dilakukan kepada seluruh akademisi maupun masyarakat pada umumnya.

Redaksi

APLIKASI SECURE-MESSAGE DENGAN ALGORITMA RC6 (RIVEST CODE 6) BERBASIS ANDROID

Arif Susanto Adhy¹, Fatsyarina Fitriastuti², Jemmy Edwin Bororing³

^{1,2,3}Program Studi Teknik Informatika Fakultas Teknik Universitas Janabadra
Jl. Tentara Rakyat Mataram No. 57 Yogyakarta 55231, Telp./Fax. (0274) 543676

E-mail: ¹basscomb88@gmail.com, ²fitri@janabadra.ac.id, ³jemmy@janabadra.ac.id

ABSTRACT

Many factors must be considered in terms of security when communicating using information technology. SMS is one of the features that are embedded in a mobile phone is no exception in android phone. SMS is still widely used for the exchange of information, many users inadvertently share information that is privacy by sending a message by SMS. Messages that are done with SMS will be received by the provider of the service provider, then after it was forwarded to the recipient therefore sending a message by SMS need to be protected, so that the safety messages are kept strictly confidential. In this study, the software will be built in order to improve the security of messages via SMS. The application will be built to encrypt a message that will be sent and decrypt incoming messages via SMS. Applications built using the RC6 algorithm. RC6 algorithm is an algorithm flow block (block cipher) were included into the type of symmetric key cryptography system. RC6 algorithm implementation is built using Android technology, to protect and maintain the confidentiality of messages. The results of trials that have been done with this application, encrypts messages sent and can decrypt a message that was well received, the message can only be decrypted if entered the correct key corresponding to the message encryption key at the time. This application can only perform encryption and decryption of text messages (letters, numbers, symbols), to encrypt the decrypted form of the image file can not be done with this application.

Keyword : SMS, Android, Cryptography, Algorithms RC6.

1. PENDAHULUAN

Perkembangan teknologi telekomunikasi yang telah ada sekarang ini mampu menciptakan bermacam macam perangkat keras yang dapat dipergunakan untuk mengirim atau menerima informasi dengan sangat mudah dan cepat. Penggunaan ponsel sebagai alat untuk mengakses informasi telah berkembang pesat. Bahkan sudah banyak aplikasi mobile pihak ketiga yang diciptakan untuk mengakses berbagai informasi dengan mudahnya. Produsen ponsel berbagai *brand*, telah banyak mengembangkan berbagai ponsel pintar khususnya perangkat dengan OS android. Ponsel android menjadi salah satu perangkat yang cukup banyak digunakan saat ini, menggantikan OS *symbian* yang telah usang dan terlebih dahulu ada. Dari sekian fitur yang ada pada android, layanan *Short Message Service* (SMS) masih sering digunakan, padahal SMS bukan merupakan jalur yang aman untuk hal pertukaran informasi. Pesan yang dikirim melalui aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi, dan pada proses pengiriman SMS tersebut tidak

langsung sampai kepada penerima, tetapi pengiriman SMS akan melewati *Short Message Service Center* (SMSC) dahulu, yang berfungsi untuk mencatat komunikasi antara pengirim dan penerima. Secara otomatis SMS akan tersimpan pada SMSC, maka operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut, hal ini terbukti dari beberapa kasus yang ditangani pihak penegak hukum, dimana pihak-pihak tersebut akan meminta transkrip SMS ke operator telekomunikasi seluler untuk dijadikan bahan penyelidikan dan sebagai bukti di persidangan. Rumusan masalah pada penelitian ini adalah sebagai berikut: a). bagaimana merancang Aplikasi *Secure-Message* dengan Algoritma RC6 (*Rivest Code 6*) supaya dapat dijalankan pada sistem operasi *mobile* android dan b). bagaimana membangun Aplikasi *Secure-Message* dengan Algoritma RC6 (*Rivest Code 6*) yang dapat dijalankan pada sistem operasi *mobile* android.

Tujuan dilakukannya penelitian ini adalah sebagai berikut:

- a. Membangun aplikasi pada perangkat android, sebagai aplikasi pihak ketiga

yang mampu melakukan enkripsi dan dekripsi data teks pada layanan SMS sebelum dan sesudah dikirimkan.

- b. Mengimplementasikan enkripsi *data* pada pengiriman pesan teks pada layanan SMS dengan metode *RC6*.

2. TINJAUAN PUSTAKA

Penelitian yang dilakukan oleh Firdaus, dkk dengan judul “Penerapan Enkripsi Pesan Rahasia untuk Pengiriman SMS Menggunakan Algoritma *Arc4* pada Peralatan Teknologi *Mobile*”. menghasilkan aplikasi yang dibangun dengan teknologi *JAVA MIDP 2.0* menggunakan program Netbean 6.8 [1]. Penelitian lain yang dilakukan oleh Hendrayanto dkk dengan judul Program Aplikasi Enkripsi Dan Dekripsi SMS Pada Ponsel Berbasis Android Dengan Algoritma *DES*, menghasilkan aplikasi *SMScrypt* dibangun menggunakan program *Eclipse* [2] Harini, dkk melakukan penelitian dengan judul Aplikasi Enkripsi SMS Dengan Modifikasi *Vigenere Cipher* pada Ponsel Android, menghasilkan aplikasi yang dibangun dengan menggunakan program *Eclipse* [3]. Perbedaan dari 3 penelitian diatas dengan yang akan peneliti kerjakan yaitu aplikasi akan dibangun dengan menggunakan pemrograman android menggunakan algoritma *RC6 (Rivest Code 6)* serta memakai *software* Android Studio, aplikasi dapat digunakan dengan mudah dengan bantuan petunjuk pemakaian pada aplikasi.

3. LANDASAN TEORI

a. Aplikasi

Aplikasi adalah pokok pembahasan yang merupakan hasil dari penggunaan atau penerapan suatu konsep. Aplikasi juga dapat disebut sebagai program komputer yang diciptakan untuk membantu dan meringankan pekerjaan manusia.

b. *Secure-Message*

Secure-Message merupakan suatu pesan yang telah dienkripsi dengan menggunakan algoritma tertentu, pesan ini hanya dapat dibaca setelah memasukkan kode kunci untuk melakukan dekripsi dari pesan tersebut, biasanya pesan yang dienkripsi tersebut merupakan pesan yang tergolong rahasia dan hanya segelintir orang yang berhak mengetahui isi dari pesan tersebut.

c. Algoritma Kriptografi

Berdasarkan jenis kunci yang dipakai, algoritma kriptografi dibagi menjadi 2 bagian yaitu :

1) Kunci Simetris

Kunci simetris adalah kunci yang digunakan pada saat membuat pesan dan digunakan juga pada saat membaca pesan. Kunci yang dimiliki pengirim dan penerima adalah sama, jadi siapapun yang mengetahui kunci tersebut, dapat membaca pesan yang telah di enkripsi. Contoh algoritma yang memakai kunci simetris diantaranya : *RC6*, *DSI*, *DS2*, *Helix* dan lainnya.

2) Kunci Asimetris

Pada kunci asimetris, konsepnya berbeda dengan kunci simetris. Pada kunci asimetris, kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda. Para pengguna yang memiliki kunci publik enkripsi bisa melakukan proses enkripsi terhadap pesan, tetapi hanya satu pengguna yang mempunyai kunci privat yang dapat melakukan proses dekripsi pesan. Contoh algoritma yang memakai kunci asimetris diantaranya : *RSA*, *DH*, *DSA* dan lainnya.

d. Kriptografi *RC6*

Menurut Fithria, kriptografi merupakan ilmu yang mempelajari teknik-teknik yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Pesan awal yang belum di enkripsi dan pesan yang telah dekripsi disebut *plaintext*, sedangkan pesan yang telah di enkripsi disebut *ciphertext*. *RC6* merupakan block cipher turunan dari *RC5*. Didesain oleh Ron Rivest, Matt Robshaw, Ray Sidney, dan Yigun Lisa Yin untuk memenuhi persyaratan kompetisi *Advanced Encryption Standard (AES)*. *RC6* mempunyai *block size* 128 bit dan mendukung dengan panjang kunci 128, 192, dan 256 bit.

e. SMS

SMS diartikan sebagai pesan singkat yang merupakan sistem sederhana dari pengiriman pesan oleh jaringan telepon seluler. SMS yang dikirim akan masuk ke dalam SMSC operator

untuk dicatat, setelah itu pesan akan otomatis diteruskan kepada penerima. Setelah pesan diterima, nomor penerima akan mengirimkan laporan bahwa pesan sudah diterima kepada SMSC, setelah dicatat otomatis laporan tadi akan dikirim kepada nomor pengirim yang disertai laporan tentang status pesan yang sudah terkirim. Begitupun sebaliknya jika penerima melakukan pengiriman pesan balik.

f. Android

Android merupakan suatu sistem operasi berbasis linux yang dikembangkan untuk perangkat bergerak, dalam hal ini adalah ponsel. Android merupakan sistem operasi dibawah kekuasaan Google dengan lisensi yang terbuka, oleh karena itu semua orang tak terkecuali dapat mengembangkan android sesuai keinginan tanpa terkendala hak cipta.

g. Android Studio

Menurut web resmi (*official*) Android Studio yaitu <https://developer.android.com>, Android Studio merupakan software yang digunakan untuk pengembangan aplikasi android, berdasarkan *IntelliJ IDEA*.

h. Java Development Kit (JDK) dan Software Development Kit (SDK)

JDK adalah perangkat lunak yang digunakan untuk melakukan pembuatan ataupun pengembangan aplikasi berbasis java, jika hanya untuk menjalankan aplikasi yang dibangun dengan java, maka JDK ini tidak diperlukan. SDK merupakan antarmuka yang menghubungkan JDK dengan Android, dengan kata lain tanpa SDK, akan mustahil membuat aplikasi berbasis android. Keduanya merupakan perangkat lunak yang tidak bisa dipisahkan dalam membangun aplikasi berbasis android.

4. METODOLOGI PENELITIAN

Tahap pembuatan aplikasi ini menggunakan metode *waterfall*. Metode *waterfall* merupakan sebuah model pengembangan perangkat lunak yang dilakukan secara sekuensial, yaitu dimana satu tahap dilakukan setelah tahap sebelumnya telah selesai dilaksanakan. Beberapa tahapan dalam metode ini dapat disajikan sebagai berikut :

a. Analisis

Pada tahap ini dilakukan analisa data sesuai dengan kebutuhan sistem yang kemudian akan diolah berdasarkan kebutuhan aplikasi.

b. Desain

Pada tahap ini dilakukan pembuatan perancangan menu aplikasi, diagram *use case* dan *flowchart* (diagram alir).

c. Coding

Pada tahap ini merupakan sebuah proses untuk merubah suatu desain menjadi sebuah bentuk yang dimengerti oleh perangkat berbasis android.

d. Testing

Pada tahap ini dilakukan untuk pengujian pada perangkat lunak dengan menggunakan perangkat android (*smartphone*) supaya lebih responsif dari pada menggunakan AVD (*Android Virtual Device*) yang kebanyakan memiliki respon yang lambat.

e. Implementasi

Pada tahap ini merupakan tahap akhir dari pengembangan aplikasi. Setelah sebelumnya melalui tahap testing, aplikasi ini diimplementasikan ke dalam perangkat android.

5. HASIL DAN PEMBAHASAN

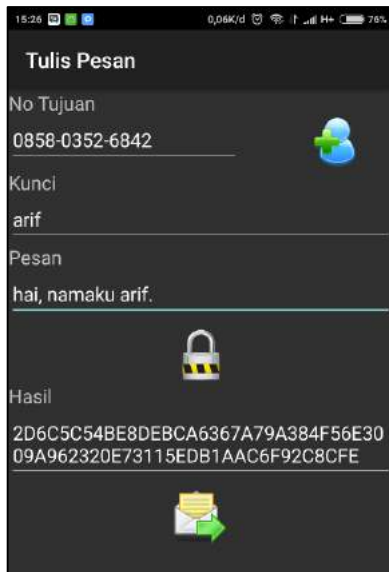
1. Pengujian dengan data pendek

a. Pengujian enkripsi

Data yang digunakan untuk proses enkripsi adalah sebagai berikut:

- Kunci
"arif"
- Pesan
"hai, namaku arif."
- Hasil
"2D6C5C54BE8DEBCA6367A79A384
F56E3009A962320E73115EDB1AAC6
F92C8CFE"

Pada gambar 1 adalah hasil enkripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 1 Pengujian enkripsi

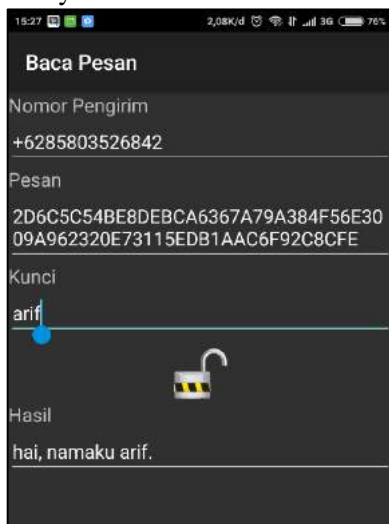
Pada gambar 1, pesan berhasil di enkripsi menjadi kumpulan huruf dan angka yang tidak beraturan dan tidak dapat dibaca, nantinya penerima pesan akan menerima pesan yang sudah di enkripsi.

b. Pengujian dekripsi dengan kunci yang benar

Data yang digunakan untuk proses dekripsi adalah sebagai berikut:

- Kunci
"arif"

Pada gambar 2 adalah hasil dekripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 2 Pengujian dekripsi dengan kunci yang benar

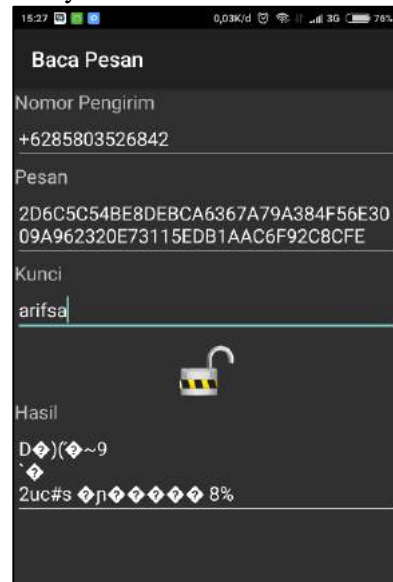
Pada gambar 2, pesan berhasil di dekripsi, karena kunci yang dimasukkan adalah benar, sehingga hasil dari pesan yang

didekripsi menjadi kumpulan kalimat yang dapat dipahami ataupun dibaca.

c. Pengujian dekripsi dengan kunci yang salah

- Kunci
"arif"

Pada gambar 3 adalah hasil dekripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 3 Pengujian dekripsi dengan kunci yang salah

Pada gambar 3, pesan tidak berhasil di dekripsi, karena memasukkan kunci yang salah atau tidak semestinya, sehingga hasil dari pesan yang didekripsi menjadi kumpulan karakter yang tidak dapat dipahami ataupun dibaca.

2. Pengujian dengan data panjang

a. Pengujian enkripsi

Data yang digunakan untuk proses enkripsi adalah sebagai berikut:

- Kunci
"universitas janabadra yogyakarta"
- Pesan
"hai, namaku arif, aku kuliah di universitas janabadra yogyakarta dan mengambil jurusan teknik informatika. ini adalah aplikasi yang aku buat untuk memenuhi tugas akhir."
- Hasil
"E33F303F8E7E4A5CEAF71D3CE6E1 CAB88E99E92346624BDFAD54DD6B 9DF0E7FAB70C7A731C2D4518CE78 B7D10C7E9113FB8CEBAEB418F8CB C89A8E364A8A0FA44AE03D81D3295"

3F902EA1BDB14DBD85A0FD360F57
 9A120CCE205864AB4A5C3916C323A
 065FCCEA3E91214007F86926117642F
 A14FCAE149DD23CA6493E9598E521
 17F77AC96B117674FC64AE16EFB96
 E2342F845BC1F5EB6B137BB289A12
 F64335B011C08145A5E14655BDFCE3
 499F50”

Pada gambar 4 adalah hasil enkripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 4 Pengujian enkripsi

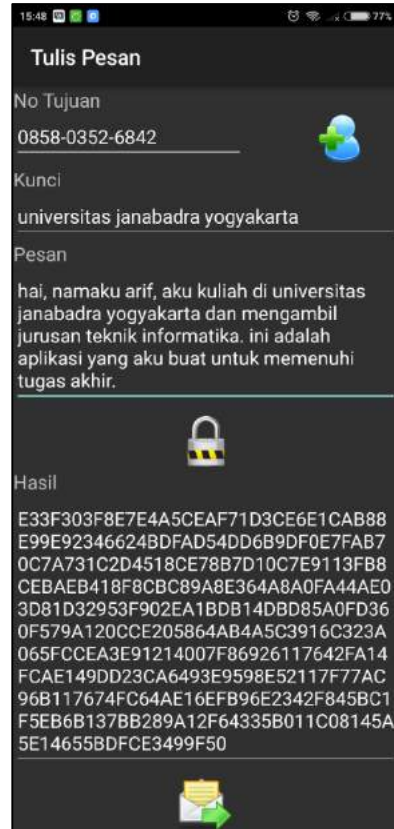
Pada gambar 4, pesan berhasil di enkripsi menjadi kumpulan huruf dan angka yang tidak beraturan dan tidak dapat dibaca, nantinya penerima pesan akan menerima pesan yang sudah di enkripsi.

b. Pengujian dekripsi dengan kunci yang benar

Data yang digunakan untuk proses dekripsi adalah sebagai berikut:

- Kunci
 “universitas janabadra yogyakarta”

Pada gambar 5 adalah hasil dekripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 5 Pengujian dekripsi dengan kunci yang benar

Pada gambar 5, pesan berhasil di dekripsi, karena kunci yang dimasukkan adalah benar, sehingga hasil dari pesan yang didekripsi menjadi kumpulan kalimat yang dapat dipahami ataupun dibaca.

c. Pengujian dekripsi dengan kunci yang salah
 Data yang digunakan untuk proses dekripsi adalah sebagai berikut:

- Kunci
 “janabadra@2012”

Pada gambar 6 adalah hasil dekripsi pesan memakai data yang sudah disebutkan sebelumnya.



Gambar 6 Pengujian dekripsi dengan kunci yang salah

Pada gambar 6, pesan tidak berhasil di dekripsi, karena memasukkan kunci yang salah atau tidak semestinya, sehingga hasil dari pesan yang didekripsi menjadi kumpulan karakter yang tidak dapat dipahami ataupun dibaca.

6. KESIMPULAN DAN SARAN

Aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*) ini diharapkan dapat membantu dan dapat digunakan sebaik mungkin dengan tidak menyalahgunakannya. Ada beberapa kesimpulan dan saran yang dapat disampaikan penulis sebagai hasil dari evaluasi pengembangan sistem, yaitu:

a. Kesimpulan

Berdasarkan dari hasil dan pembahasan pengujian aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*), maka dapat diambil kesimpulan :

- Penelitian ini berhasil membangun aplikasi enkripsi SMS pada *smartphone* berbasis android menggunakan algoritma *RC6* (*Rivest Code 6*).
- Aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*) ini dirancang dengan

menggunakan bahasa pemrograman *java* menggunakan *software* Android Studio.

- Aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*) ini dapat di implementasikan pada sistem operasi android versi 4.2.2 ke atas.
- Berdasarkan pada hasil pengujian yang dilakukan, aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*) ini dapat melakukan enkripsi dan dekripsi SMS dengan baik.

b. Saran

Pada saat proses pengembangan aplikasi *secure-message* dengan algoritma *RC6* (*Rivest Code 6*) ini, ada beberapa saran yang harus diterapkan guna pengembangan lebih lanjut yaitu :

- Aplikasi ini hanya dapat mengirim pesan data teks berupa huruf, angka dan simbol, sehingga untuk pengiriman gambar belum bisa dilakukan.
- Pesan yang dikirim oleh aplikasi setelah enkripsi SMS menjadi lebih panjang.
- Apabila jumlah iterasi (iterasi digunakan untuk melakukan rotasi algoritma *RC6*) semakin besar, maka tingkat keamanan akan semakin baik, tetapi waktu yang dibutuhkan juga akan semakin besar untuk melakukan proses enkripsi maupun dekripsi pesan.

DAFTAR PUSTAKA

- Afriandinata, D. N., Inayatullah, Hanafi, J., 2015, *Secure Text Message Dengan Metode Enkripsi Dekripsi Algoritma Rc6 Berbasis Android*, STMIK MDP, Palembang.
- Hanafi, J., Hartatik, 2016, *Perancangan Pesan Rahasia Aplikasi Sms Menggunakan Algoritma Rc6 Berbasis Android (Studi Kasus: Pt. Time Excelindo)*, STMIK Amikom, Yogyakarta.
- Firdaus, R., Damanik, R., Kurniawan, D., 2010, *Penerapan Enkripsi Pesan Rahasia untuk Pengiriman Sms Menggunakan Algoritma Arc4 pada Peralatan Teknologi Mobile*, Program Studi Ilmu Komputer Jurusan Matematika Universitas Lampung, Lampung.
- Fithria, N., 2007, *Jenis-Jenis Serangan Terhadap Kriptografi*, Jurusan Teknik Informatika ITB, Bandung.

Hanafi, J., Hartatik, 2016, *Perancangan Pesan Rahasia Aplikasi Sms Menggunakan Algoritma RC6 Berbasis Android (Studi Kasus: PT. Time Excelindo)*, Jurusan Teknik Informatika STMIK Amikom, Yogyakarta.

Harini, R. T., Utami, E., 2012, *Aplikasi Enkripsi Sms Dengan Modifikasi Vigenere Cipher Pada Ponsel Android*. STMIK Amikom, Yogyakarta.

Hendrayanto, R., Nilawati, A. R., 2012, *Program Aplikasi Enkripsi Dan Dekripsi Sms Pada Ponsel Android Dengan Algoritma DES*. Jurusan Sistem Informasi, Fakultas Ilmu Komputer, Universitas Gunadarma, Depok.

Mukodim, D., 2002, *Tinjauan Tentang Enkripsi Dan Dekripsi, Suatu Teknik Pengamatan Data Dengan Penyandian RSA*, Universitas Gunadarma, Depok.