# IMPLEMENTASI METODE RC6 UNTUK KEAMANAN PESAN BERBASIS ANDROID

Suci Ananda Sari[1], Wiwien Hadikurniawati[2]
Universitas Stikubank Semarang[12]
Jln. Tri Lomba Juang No.1, Kota Semarang, Jawa Tengah
Email : sucianandasari29@gmail.com[1], wiwien@edu.unisbank.ac.id[2]

***ABSTRAK***

Keamanan pesan dalam berkomunikasi menggunakaan telepon atau smartphone sangatlah penting. Mengingat isi atau data dalam pesan tersebut sangatlah rahasia. Perkembangan teknologi telekomunikasi di era gobalisasi yang terjadi sangat pesat membantu masyarakat untuk komunikasi dan salah satu teknologi komunikasi adalah menggunakan perangkat telepon. Telepon genggam atau smartphone telah dilengkapi dengan berbagai fitur dan salah satu diantaranya adalah layanan pesan singkat (SMS). Akan tetapi pesan yang dikirim melalui telepon atau smartphone yang dirasa adalah data yang sangat penting dapaat menimbulkan ancaman kebocoran isi data dalam pesan tersebut saat melakukan proses komunikasi. Maka dari itu, perlu dilakukan penelitian pada pengembangan perangkat lunak untuk meningkatkan keamanan pesan melalui enkripsi dan dekripsi. Penelitian ini dilakukan untuk menganalisis keamanan dengan mengimplementasikan algoritma RC6 pada aplikasi kriptografi dan SMS berbabsis android. Aplikasi ini menggunakan Android Studio 4.0 sebagai editor dan algoritma RC6. Proses dari penelitian ini adalah melakukan enkripsi pesan asli untuk menghasilkan ciphertex pesan. Kemudian mendekripsi ciphertext pesan masuk menjadi pesan asli. Dengan penerapan kriptografi untuk pesan SMS , tingkat informasi yang diharapkan keamanan pesan dapat ditingkatkan sehingga pesan akan lebih aman dari akses yang tidak sah atau tidak bertanggung jawab. Serta memberi rasa nyaman dan tidak khawatir akan kebocoran isi pesan tersebut oleh pengirim kepada penerima pesan.

Kata kunci : Android, Dekirpsi, Enkripsi, RC6, SMS.

***ABSTRACTS***

*Message security in communicating using a phone or smartphone is very important. Given the content or data in the message is very confidential. The development of telecommunications technology in the era of globalization that occurs very rapidly helps people to communicate and one of the communication technologies is using telephone devices. Mobile phones or smartphones have been equipped with various features and one of them is a short message service (SMS). However, messages sent via telephone or smartphone that are considered very important data can pose a threat of leakage of data content in the message during the communication process. Therefore, it is necessary to do research on software development to improve message security through encryption and decryption. This research was conducted to analyze security by implementing the RC6 algorithm on android-based cryptography and SMS applications. This application uses Android Studio 4.0 as editor and RC6 algorithm. The process of this research is to encrypt the original message to produce a message ciphertex. Then decrypt the ciphertext of the incoming message into the original message. With the application of cryptography for SMS messages, the level of information expected for message security can be increased so that messages*

*will be more secure from unauthorized or irresponsible access. As well as giving a sense of comfort and not worrying about the contents of the message leaking by the sender to the recipient of the message.*

*Keywords: Android, Decryption, Encryption, RC6, SMS.*

## 1. PENDAHULUAN

Perkembngan teknologi yang terjadi saat ini telah mengubah cara masyarakat dalam berkomunikasi. Dengan adanya teknologi telepon atau smartphone memudahkan masyarakat dalam pertukaran informasi. Tetapi dalam perkembangan teknologi ini juga memiliki kelemahan dalam hal keamanan data. Misalnya penyadapan data yang dapat dilakukan oleh pihak-pihak yang tidak bertanggung jawab dan menyalahgunakan isi data tersebut. Oleh karena itu perlu digunakannya kriptografi. Kriptografi ini bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Kriptografi berasal dari Bahasa Yunani, yang terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi mempelajari teknik matematikan yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data,integritas data, dan autentikasi data[1].

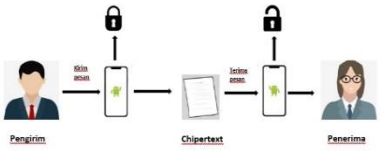
Algoritma RC6 merupakan salah satu kandidat Advanced Encryption Standard (AES) yang diajukan oleh RSA Security Laboratories kepada NIST. Dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin, algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST. RC6 adalah algoritma yang menggunakan ukuran blok hingga 128 bit, dengan ukuran kunci yang diguankan bervariasi antara 128, 192 dan 256 bit[2].

Algoritma RC6 adalah versi yang dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b, dimana parameter w merupakan ukuran kata dalam satuan bit, r adalah bilangan bulat bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam byte.
[3].

## 2. METODE PENELITIAN

Pada penelitian ini metode yang digunakan adalah metode RC6 dan menggunakan algoritma enkripsi dan dekripsi. Pada proses enkripsi ciphertex yaitu dengan menggunakan operasi penjumlahan, sedangkan pada proses deskripsi yaitu menggunakan operasi pengurangan.

### 2.1 Deskripsi Umum Sistem




Gambar 1. Deskripsi Umum Sistem

Pada gambar diatas terlihat proses dari pengirim membuat dan mengirim pesan kepada penerim. Tetapi sebelum pesan diterima oleh penerima , pesan akan terlebih dahulu mengalami proses enkripsi dengan menggunakan kunci dan pesan yang terenkripsi akan menghasilkan ciphertext. Kemudian untuk medeskripsikan ciphertext tersebut, penerima harus memasukkan kunci dahulu agar bisa menjadi plaintext dan bisa dibaca oleh penerima isi pesan tersebut.

### 2.2 Metode Algoritma RC6

Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter merupakan bilangan bukan negatif yang menunjukan banyaknya

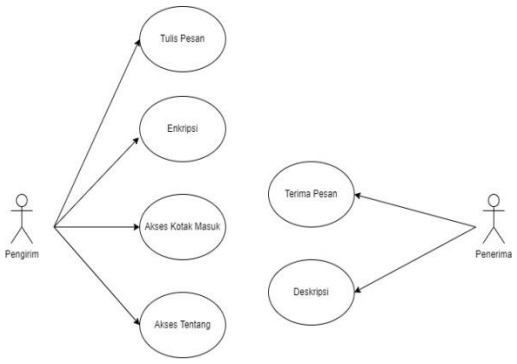
iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte. Setelah algoritma ini masuk dalam kandidat AES, maka ditetapkan bahwa nilai w = 32, r=20 dan b bervariasi antara 16, 24 dan 32 byte.
RC6-w/r/b memecah blok 128 bit menajdi 4 buah blok 32-bit, dan mengikuti aturan enam operasi dasar sebagai berikut :

1. A + B Operasi penjumlahan bilangan integer.
2. A – B Operasi pengurangan bilangan integer.
3. A B Operasi exclusive-OR (XOR)
4. A x B Operasi perkalian bilangan integer.
5. A<<>>B A dirotasikan ke kanan sebanyak variabel kedua (B)
6. A>>>B A dirotasikan ke kanan sebanyak variabel kedua (B)

## 3. HASIL DAN PEMBAHASAN

Aplikasi kriptografi untuk keamanan pesan berbasis android ini dibuat dan diimplementasikan guna membantu user atau penerima pesan untuk menjaga kerahasiaan isi pesan tersebut.

### 3.1 Diagram Use Case




Gambar 2. Diagram Use Case

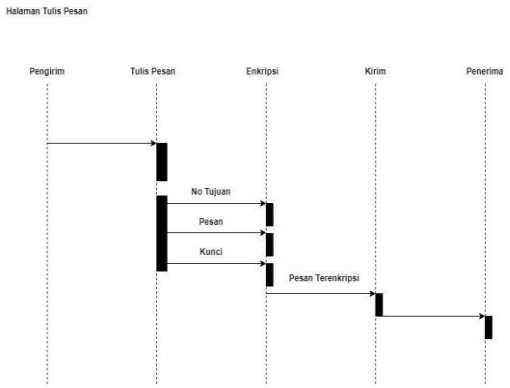
Pada gambar diagram use case diatas mendeskripsikan atau menjelaskan sebuah interaksi antara pengirim dan penerima, serta menjelaskan cara kerja pada aplikasi keamanan pesan tersebut.

### 3.2 Spesifikasi Use Case

| Aktor | Deskripsi |
|---|---|
| Pengirim | Tulis Pesan<br>Pengirim menulis pesan pada aplikasi untuk dikirim |
| Pengirim | Enkripsi Pesan<br>Pengirim mengenkripsi pesan yang akan dikirim agar pesan teracak dan tidak dapat dibaca |
| Pengirim/ Penerima | Akses Kotak Masuk<br>Pengirim/penerima membaca pesan didalam kotak masuk |
| Penerima | Terima Pesan<br>Penerima mendapatkan pesan dari pengirim |
| Penerima | Deskripsi Pesan<br>Penerima mendeskripsi pesan yang teracak agar tidak terbaca |
| Pengirim/ Penerima | Akses Tentang<br>Pengirim/Penerima mendapat keterangan mengenai aplikasi seperti versi dan pembuat aplikasi |

Tabel 1. Tabel spesifikasi use case

### 3.3 Diagram Squence Enkripsi



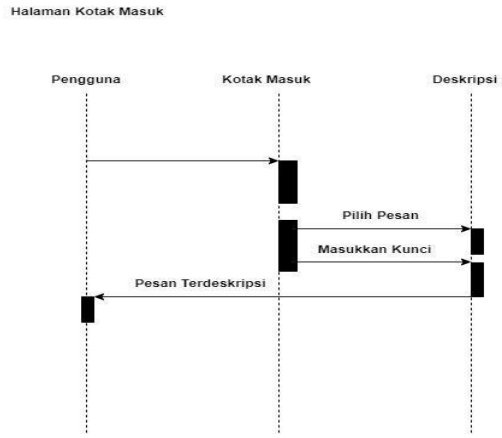

Gambar 3. Diagram sequence enkripsi.

Deskripsi dari diagram sequence enkripsi diatas yaitu pengirim memilih pada opsi tulis pesan

*P-ISSN: 2337-8344*
*E-ISSN: 2623-1247*

kemudian pengirim memasukkan no tujuan, pesan yg akan dikirim dan kunci, kemudian secara otomatis pesan akan terenkripsi dan diteruskan ke penerima.

### 3.4 Diagram sequence deskripsi

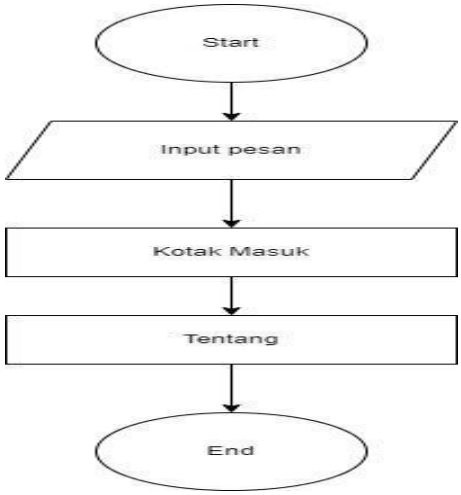



Gambar 4. Diagram sequence deskripsi

Deskripsi dari diagram sequence deskripsi diatas yaitu pengguna memilih pesan yang masuk kemudian memasukkan kunci, dan secara otomatis pesan akan terdeskripsi dan dapat terbaca.

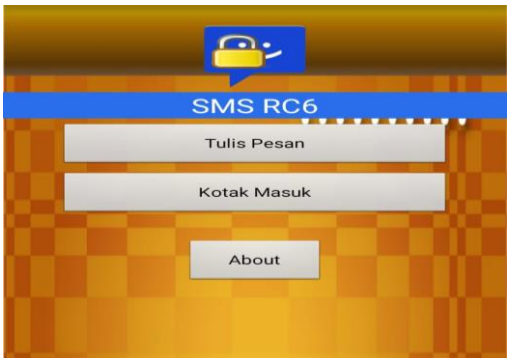
### 3.5 Implementasi

1. Tampilan Utama




Gambar 5. Flowchart taampilan utama

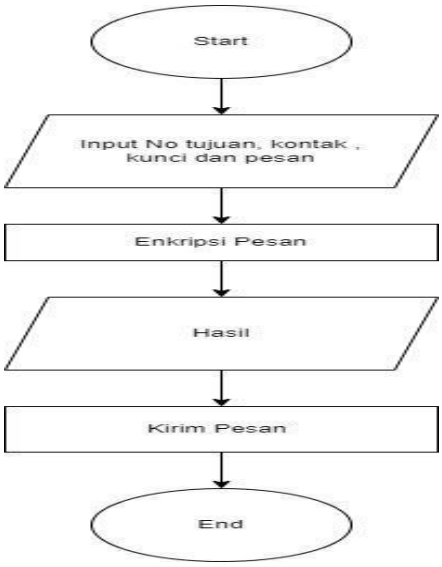
Gambar flowchart diatas merupakan flowchart dari tampilan utama yang dilakukan start kemudian terlihat menu input pesan, kotak masuk dan tentang dan end.




Gambar 6. Tampilan Utama

Gambar pada menu "Tampilan Utama" diatas adalah tampilan utama dari sistem keamanan berbasis android yang berisikan tulis pesan, kotak masuk, dan about.

2. Tampilan Tulis Pesan




Gambar 7. Flowchart tulis pesan.

Gambar flowchart diatas merupakan flowchart dari Tulis Pesan yang pertama start kemudian masukkan no tujuan, kontak, kunci dan pesan, setelah itu proses enkripsi pesan. Setelah di

*P-ISSN: 2337-8344*
*E-ISSN: 2623-1247*

enkripsi akan muncul hasil pesan setelah enkripsi kemudian bisa dipilih kirim pesan dan end atau selesai.


Gambar 8. Gambar tulis pesan.

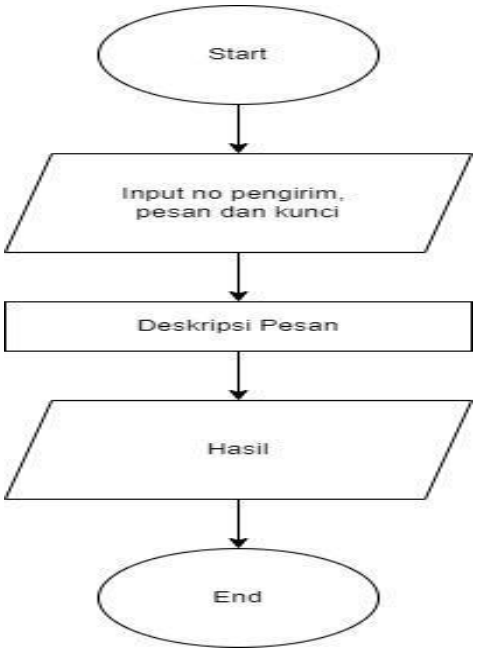
Dari gambar 8 diatas jika button "Tulis Pesan" diklik akan muncul beberapa data yang akan dimasukkan untuk proses mengirimkan pesan. Data yang harus dimasukkan adalah no tujuan, kunci, dan pesan.

Kemudian jika sudah diisi akan tampil seperti gambar dibawah terlihat proses atau aktivitas saat memasukkan data data yang diperlukan untuk mengirim pesan. Yaitu memasukkan kontak penerima memasukkan kunci , dan memasukkan

pesan yang akan dikirim. Setelah memasukkan pesan yang akan dikirim kemudian pilih button kriptografi kemudian akan muncul hasil pesan yang sudah enkripsi. Jika sudah pilih kirim pesan.

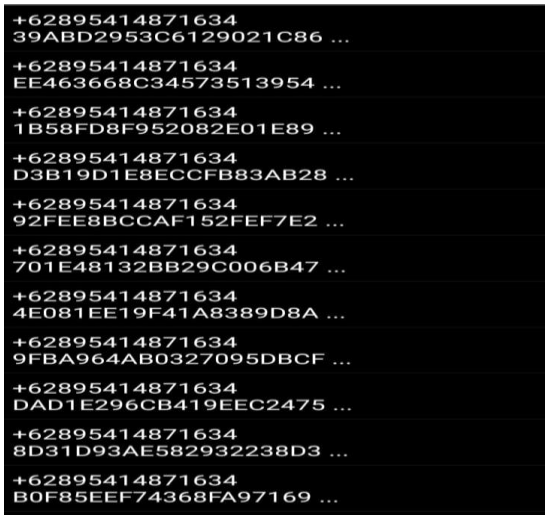

Gambar 9. Proses pengisian pesan

3. Tampilan Kotak Masuk




Gambar 10. Flowchart kotak masuk

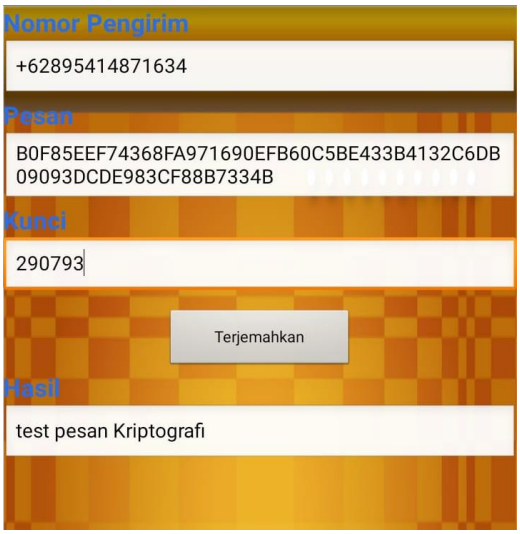
Gambar diatas merupakan flowchart dari Kotak Masuk yang dimulai dari start, kemudian mengisikan no pengirim, pesan dan kunci kemudian lakukan deskripsi pesan ,setelah dari deskripsi pesan akan muncul hasil pesan setelah dideskripsi dan selesai.




Gambar 11. Hasil kotak masuk

*P-ISSN: 2337-8344*
*E-ISSN: 2623-1247*

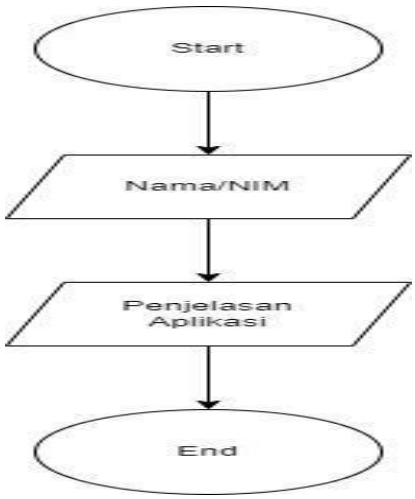
Dari Gambar diatas terlihat saat membuka kotak masuk akan tampil beberapaa pesan yang sudah dienkripsi sehingga siapaun yg membaca kecuali penerima yang sah tidak akan mengetahui apa isi pesan tersebut.




Gambar 12. Hasil dekripsi pesan masuk

Kemudian dari gambar 12 diatas pilih salah satu pesan kemudian maasukkan kunci dan pilih terjemahkan atau dekripsi agar mengetahui isi dari pesan tersebut.

4. Tampilan About




Gambar 13. Flowchart about.

Gambar diatas merupakan flowchart dari about yang dimulai lalu terdapat nim/nama serta penjelasan tentang aplikasi kemudian proses selesai.


Gambar 14. Tampilan about.

Berisikan tentang tujuan aplikasi tersebut dibuat dan informasi mengenai pembuat aplikasi tersebut sesuai yang terlihat pada gambar 14.

## 4. KESIMPULAN

Hasil akhir dari penelitian ini dapat dilihat dari beberapa proses yang dijelaskan diatas adalah terbentuknya sebuat sistem aplikasi keamanan pesan berbasis android dengan metode RC6 yang membantu user atau penerima pesan untuk mengamankan serta merahasiakan isi dari pesan tersebut dengaan kriptografi. Sehingga memperkecil terjadinya kebocoran isi pesan kepada pihak-pihak yang tidak bertangguh jawab sesuai yang diharapkan.

## DAFTAR PUSTAKA

[1] Ariyus D, "Kriptografi Keamanan Data dan Kriptografi", Yogyakarta : Penerbit Andi Offset, 2006.

[2] Abdurohman, Maman, "Analisis Performansi Algoritma Kriptografi RC6", Institut Teknologi Bandung, 2002.

[3] Yudi, Idham, "Jurnal Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data", Universitas Islam Indonesia, 2005.

[4] Defini I.R, "Enkripsi SMS (Short Message Service) pada Telepon Seluler Berbasis Android Dengan Metode RC6", J.Momentum 16,2014.

[5] Safaat N, "Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android", Bandung : Informatika, 2012.

[6] Muharini A, "Aplikasi Algoritma Rivest Code 6 dalam Pengamanan Citra Digital", Universitas Indonesia, 2012.

[7] Permana, "Implementasi Algoritma RC6 Untuk Enkripsi SMS Pada Telepon Selular", Institut Teknologi Bandung, 2008.

[8] R.Presman, "Rekayasa Perangkat Lunak", Yogyakarta : ANDI, 2012.

[9] Tantra, "Manajemen Proyek Sistem Informasi", Yogyakarta : ANDI, 2012.

[10] Roland, "Jurnal Perbandingn Algoritma Block Ciher R5 dan RC", Institiut Teknologo Bandung , 2006