IMPLEMENTASI ALGORITMA RIVEST CODE (RC6) PADA APLIKASI KEAMANAN DATA SMS BERBASIS ANDROID

Anggi Puspita Sari [1], Muhamad Panca Mustika[2], Raudah Nasution [3], Wawan Gunawan[4],

[1,3] Program Studi Sistem Informasi, Universitas Bina Sarana Informatika
[2] Program Studi Teknik Informatika Universitas Nusa Mandiri Jakarta
[4]Program Studi Teknik dan Informatika Universitas Mercubuana
Jl. Kramat Raya No 98, Jakarta Pusat

anggi.apr@bsi.ac.id, panca.mpm@gmail.com, raudah.rhn@bsi.ac.id, wawan.gunawan@mercubuana.ac.id

ABSTRACT

Data security is a very priority in maintaining the confidentiality of information, especially those containing sensitive information, such as in short messages containing PIN numbers and passwords that must not be known by any party except those who are entitled. However, the security of message data is not infrequently considered by users to be something that is not considered and prioritized. The use of SMS in sending messages that are confidential in nature can be intercepted by anyone because when the message is sent it will be stored in the SMSC (Short Message Service Center), which is the place where the SMS is stored before being sent to the destination. As a result, confidential messages such as pin numbers, passwords, access codes, and others can be read by parties who are not entitled to know. Therefore, using cryptography provides guarantees for the security of data or information by means of encryption and decryption using the Rivest Code (RC6) algorithm. The application of the RC6 algorithm allows SMS users to provide a key to those who have the right to open sms and make SMS safe because it cannot be accessed by unauthorized parties. The RC6 algorithm can also be used for mobile-based applications because in addition to being very simple, RC 6 is also easy to implement on android-based phones, because this algorithm only requires a small memory.

Keywords: SMS, cryptography, RC6

ABSTRAK

Keamanan data adalah hal yang sangat diutamakan dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif, seperti pada pesan singkat yang berisi nomor PIN dan Password tidak boleh diketahui oleh pihak manapun kecuali yang berhak saja. Namun keamanan data pesan tidak jarang dianggap oleh pengguna merupakan hal yang kurang diperhatikan dan diutamakan. Penggunaan SMS dalam mengirim pesan yang sifatnya rahasia dapat disadap oleh siapa saja karena pada saat pesan dikirimkan akan disimpan di SMSC (Short Message Service Center), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Akibatnya pesan yang rahasia seperti nomor pin, password, kode akses, dan lain-lain dapat dibaca oleh pihak yang tidak berhak untuk mengetahuinya. Oleh karena itu, dengan menggunakan kriptografi memberikan jaminan keamanan data atau informasi dengan cara enkripsi dan dekripsi menggunakan algoritma Rivest Code (RC6). Penerapan algoritma RC6 membuat pengguna SMS dapat memberikan kunci kepada yang berhak membuka sms dan membuat SMS menjadi aman karena tidak bisa diakses oleh pihak yang tidak diotorisasi. Algoritma RC6 juga dapat digunakan untuk aplikasi berbasis mobile karena selain sangat sederhana RC 6 juga mudah untuk diimplementasikan pada ponsel berbasis android, karena algoritma ini hanya membutuhkan memory yang kecil.

Kata Kunci: SMS, kriptografi, RC6

I. PENDAHULUAN

Keamanan data adalah hal yang sangat diutamakan dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif, seperti pada pesan singkat yang berisi nomor PIN dan Password tidak boleh diketahui oleh pihak manapun kecuali yang berhak saja. Namun keamanan data pesan tidak jarang dianggap oleh pengguna merupakan hal yang kurang diperhatikan dan diutamakan.

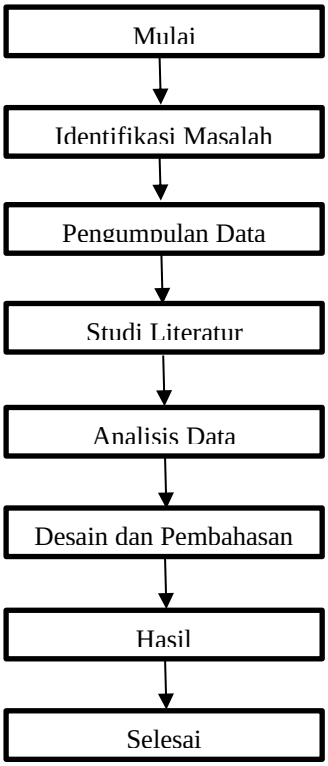
Pesan yang dikirim masih berupa teks terbuka yang belum terlindungi atau terproteksi selain itu pengiriman SMS yang dilakukan tidak sampai secara langsung ke tujuan, akan tetapi pengiriman SMS harus melewati *Short Message Service Center* (SMSC) yang memiliki fungsi mencatat segala aktifitas komunikasi yang terjadi antara pengirim dan penerima. Dengan tersimpannya SMS pada SMSC, maka pihak operator atau mungkin pihak lain yang tidak berhak mengetahui informasi tersebut tanpa sepengetahuan pengirim dapat membaca, mengambil, dan merubah isi informasi SMS yang biasa dikenal dengan istilah penyadapan di dalam SMSC.

Berdasarkan jurnal (jurnal Sulaiman R, Vebu M. (2018) Masalah keamanan dan kerahasiaan data dan informasi merupakan suatu hal yang sangat penting. Salah satu cara menjaga keamanan dan kerahasiaan data dan informasi adalah dengan teknik enkripsi dan dekripsi atau yang dikenal juga dengan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kemanan pesan dengan cara mengubahnya menjadi suatu bentuk yang tidak dapat dikenali lagi.

Untuk meminimalisir resiko tersebut, salah satu solusinya adalah menerapkan suatu algoritma kriptografi dengan terenkripsinya pesan yang akan dikirimkan. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (*plaintext*) menjadi data yang tersembunyi (*ciphertext*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan untuk megistilahkan enkripsi adalah *"enchiper"*, sedangkan untuk dekripsi adalah *"dechiper"*.

II. METODE PENELITIAN

Metode penelitian memegang peranan penting dalam memberikan pondasi atau landasan terhadap tindak dan keputusan dalam membangun suatu bidang terutama dalam sebuah penelitian. Adapun metode penelitian yang penulis gunakan untuk menyelesaikan berbagai masalah yang terjadi adalah:



Gambar 1 : Tahapan Metode Penelitian

Tahapan Metode Penelitian

Identifikasi Masalah

Pada tahapan ini masalah yang ada yaitu saat mengirimkan sms atau pesan dengan menggunakan fasilitas sms maka terdapat celah untuk seseorang dapat menyadap atau bahkan mengambil data pada pesan yang dikirimkan, karena pesan yang dikirimkan akan terlebih dahulu dikirmkan ke pesan center (SMSC) setelahnya penerima dapat membaca pesan yang dikirmkan.

Pengumpulan Data

Sesuai dengan masalah yang didapatkan maka data yang dikumpulkan adalah data-data terkait proses pengiriman SMS mulai dari SMS dikirim hingga SMS tersebut sampai ke pihak yang diotorisasi untuk membaca pesan. Selain itu juga ditentukan metode algoritma apa yang baik untuk keamana SMS.

Studi Literatur

Studi literatur yang sesuai dengan pengumpulan data yang dilakukan yaitu dengan mengumpulkan literatur dari ebook, jurnal, buku dan tulisan-tulisan pada media teknologi terkait dengan pengamanan data pada pesan SMS dan pemilihan algoritma rivest yang digunakan untuk pengamanan data tersebut.

Analisis Data

Tahapan analisis data pengamanan data pesan pada SMS sesuai dengan kebutuhanya. Data yang dianalisa adalah metode algoritma rivest code yang akan digunakan, kebutuhan aplikasi yang dapat berjalan di smartphone berbasis android dan kebutuhan data user terkait pengiriman pesan.

Desain dan pembahasan

Software Architecture yang digunakan untuk aplikasi ini menggunakan UML dan pemrograman yang digunakan adalah *java* sehingga adanya *class-class* dan atribut-atribut yang akan dipakai didalam aplikasi. Sedangkan untuk *user interface* penulis membuat didalam aplikasi ini terdapat tombol –tombol yang digunakan untuk memilih dan pembahasan terkait algoritma rivest code yang digunakan pada pengamanan data pesan pada saat pengiriman SMS.

Hasil

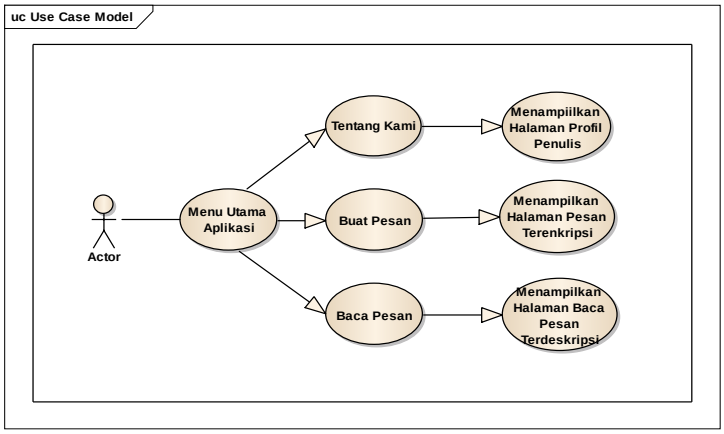
Pengujian hasil pengamanan data pesan di AVD (*Android Virtual Device*) tidak ada kesalahan, maka penerapan selanjutnya diinstal dalam sebuah *handphone / smartphone* yang berbasis *android*.

III. HASIL DAN PEMBAHASAN

Berdasarkan hasil analisa tentang kebutuhan-kebutuhan yang diperlukan, maka dapat diidentifikasikan serta diimplementasikan melalui rancangan sistem, serta rancangan layar.

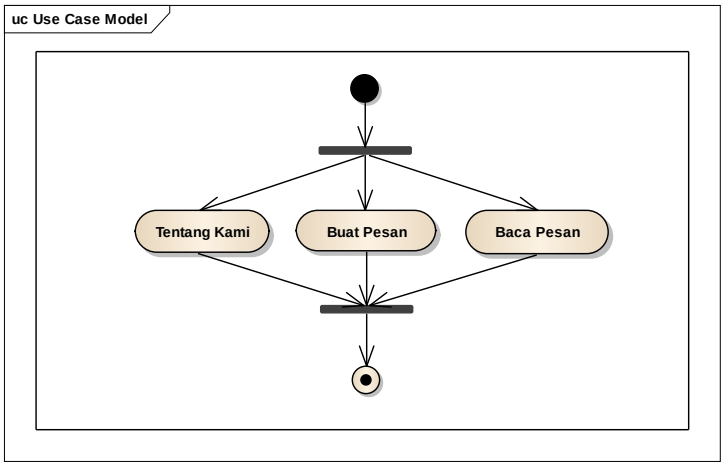
Rancangan Sistem

Use Case Diagram



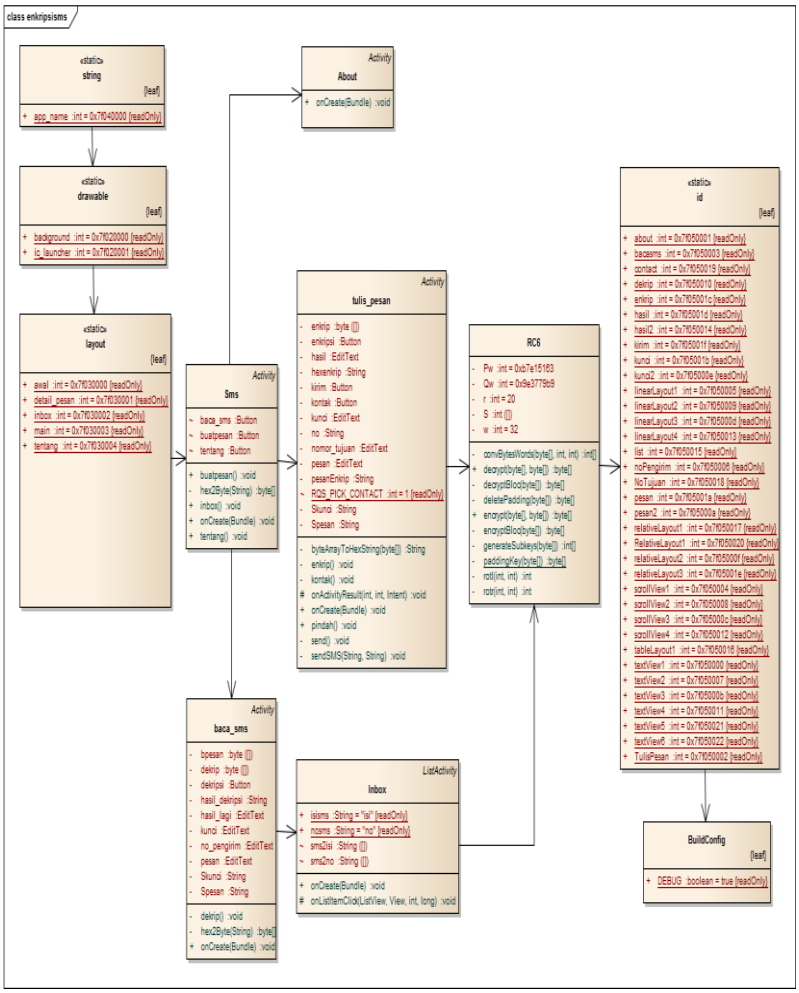
Gambar 2. *Use Case* Diagram
Sumber : Hasil Penelitian

Activity Diagram Aplikasi



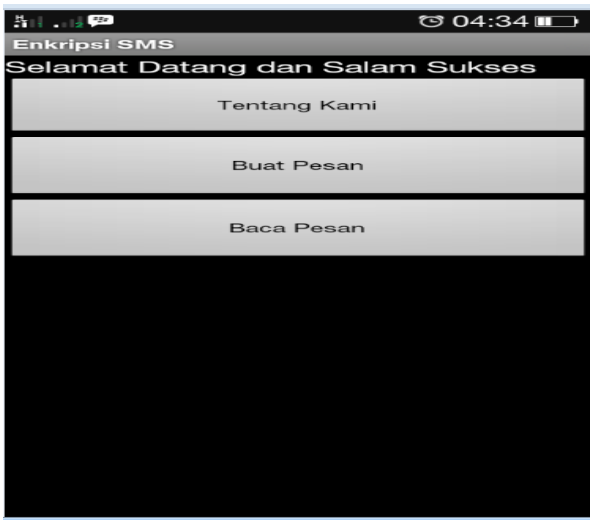
Gambar 3. *Activity* Diagram Aplikasi
Sumber : Hasil Penelitian

Class Diagram Aplikasi



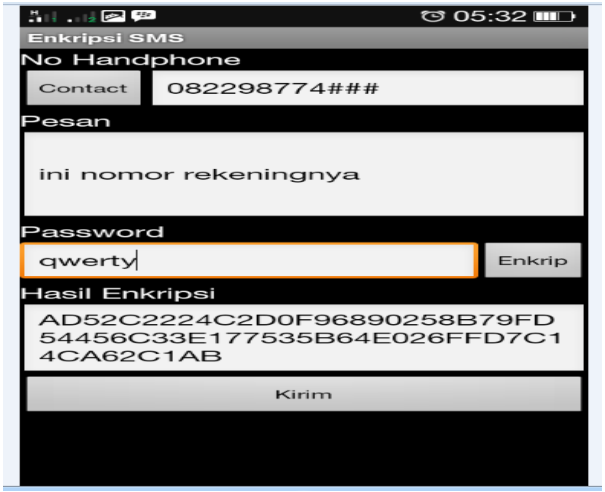
Gambar 4. *Class* Diagram Aplikasi
Sumber : Hasil Penelitian

Rancangan Layar



Gambar 5. *User Interface* Menu Utama
Sumber : Hasil Penelitian

Pada gambar 5 adalah tampilan user interface menu utama aplikasi Enkripsi SMS, terdiri atas menu tentang Kami, Menu Buat Pesan, dan Menu Untuk Membaca Pesan.



Gambar 6. *User Interface* Menu Buat Pesan
Sumber : Hasil Penelitian

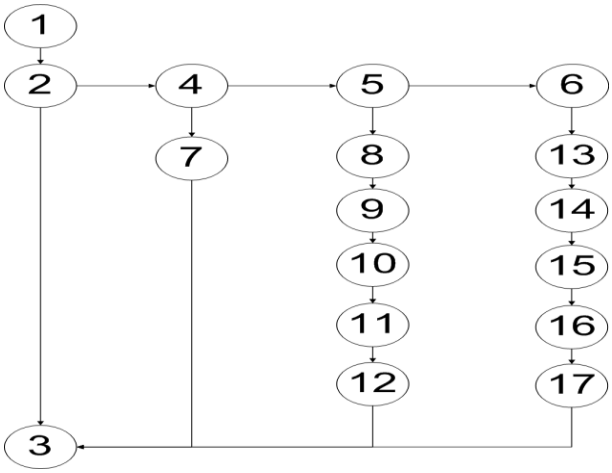
Pada Menu Buat Pesan, User membuat pesan yang akan dikirimkan dengan memasukan no telepon yang dituju, ketik isi pesan dan mengetikan password yang akan digunakan dan dilakukan enkrip dengan menggunakan algoritma rivest code.

Gambar 7. *User Interface* Menu Baca Pesan
Sumber : Hasil Penelitian

Hasil SMS yang telah dikirimkan dapat dilihat dari gambar 7. Hasil sms yang diterima dalam bentuk pesan terenkrip, untuk melihat pesan, user harus mengetikan kunci pembuka kemudian dan pesan asli dapat dilihat.

Testing

White Box



Gambar 9. *White Box*
Sumber : Hasil Penelitian

Kompleksitas Siklomatis (pengukuran kuantitatif terhadap kompleksitas logis suatu program) dari grafik alir dapat diperoleh dengan perhitungan :

Dimana :

$$V(G) = E - N + 2$$

E = Jumlah *edge* grafik alir yang ditandakan dengan gambar panah
N = Jumlah simpul grafik alir yang ditandakan dengan gambar lingkaran
V(G) = Jumlah *Region* Sehingga kompleksitas siklomatisnya
V(G) = (19 -17) + 2 = 4
V(G) < 10 berarti memenuhi ke kompleksitasi siklomatisnya.

Baris set yang dihasilkan dari jalur *independent* adalah sebagai berikut :
= 1-2-3
= 1-2-4-7-3
= 1-2-4-8-9-10-11-12-3
= 1-2-6-13-14-15-16-17-3

Black Box

Pengujian selanjutnya dilakukan untuk memastikan bahwa suatu *event* atau *input* menjelaskan proses yang tepat dan menghasilkan *output* yang sesuai dengan rancangan yang telah dibuat, berikut hasil pengujian *black box* untuk aplikasi ini.

Tabel 1. Tabel Pengujian *Black Box* Menu Buat Pesan

Deskripsi	Prosedur Pengujian	Input	Hasil Yang Di Harapkan	Hasil Yang didapat	Kesimpulan
Mengisi Form Buat Pesan	Menulis Pesan	Pesan yang akan dikirim	Dapat mengisi seluruh inputan di form tulis pesan	Form tulis pesan dapat terisi oleh inputan dari user	Diterima
	Masukkan Password		Menampilkan kunci password	Password di dapatkan	Diterima
	Enkripsi Pesan	Pesan yang Akan Dikirim	Menampilkan password dan hasil enkripsi	Password untuk enkripsi didapatkan dan proses enkripsi berjalan	Diterima
	Mengirim pesan		Pesan terkirim ke Penerima	Penerima mendapat notifikasi pesan masuk	Diterima

Sumber : Hasil Penelitian

IV. KESIMPULAN

Berdasarkan hasil penulisan yang telah dilakukan dapat disimpulkan adalah Aplikasi ini telah berhasil dijalankan pada *smartphone* berbasis *android*. Dengan adanya aplikasi keamanan data SMS memberikan jaminan terhadap kerahasiaan data. Algoritma Rivest Code 6 (RC6) berjalan dengan baik dimana pengguna hanya bisa membuka SMS dengan menggunakan kunci yang telah diberikan oleh pengirim pesan yang terotentikasi.

REFERENSI

Adhy Arif S, Fitriastuti F, Bororing Jemmy E. (2019). Aplikasi Secure-Message dengan Algoritma RC6 (rivest code 6) berbasis android. *Jurnal Informasi Interaktif*. Vol. 4 No. 2 Mei 2019. ISSN : 2527-5240

Admin. (2021) "Sistem Keamanan Data" retrieved from :
[http://www.academia.edu/7612178/SISTEM_KEAMANAN_DATA]

Juliansyah Eko. (2017). Implementasi Algoritma Kriptografi RC -6 dalam Mengamankan Data Teks. *Jurnal Pelita Informatika*. Vol. 06, No. 01. 88-90, Juli 2017 ISSN : 2301-9425

Kristianto B.D, Gat, Syarifudin G. (2020). Perancangan Perangkat Lunak Enkripsi SMS Menggunakan Algoritma RC6 Dan Rijndael Pada Smartphone, Jurnal Ilmiah SISFOTENIKA, Vol. 10, No. 1, Januari 2020

Rahman F, Wati L, Satria D. (2018). Aplikasi Keamanan Smartphone Berbasis Android Menggunakan Short Message Service. *Jaringan Sistem Informasi Robotik* Vol. 2, No. 01, Maret 2018

Rivest L, Ronald., Robshaw, M.J.B., Sidney,R., and Yin,Y.L. The RC6 Block Chiper, san Mateo, USA : RSA Laboratories, 1998. retrieved from www.rsasecurity.com/rsalabs/rc6/

Saleh R, Imelda I. (2018). Kriptografi Email menggunakan Algoritma Rivest Code 6 (Rc6) berbasis Java Pada PT. XYZ. *Seminar Nasional Sistem Informasi dan Teknologi Informasi (SENSITEK 2018)*

Safaat, Nazaruddin, 2012, Pemrograman Aplikasi Mobile smartphone dan Tablet PC Berbasis android, Penerbit Informatika, Bandung.

Sofyan H.M, Fahmi H. (2022), Implementasi Algoritma RC6 dalam Pengamanan File pada BP2RD SU Samsat Sei Rampah. *Jurnal Sistem Informasi Kaputama (JSIK).* Vol.6, No.1. Januari 2022. ISSN : 2685-5232

Sulaiman R, Vebu M. (2018). Peningkatan Keamanan Pesan Berbasis Android Menggunakan Algoritma Kriptografi RSA. *Jurnal SISFOKOM*. Vol.07, No.02. Sept 2018.http://dx.doi.org/10.32736/sisfokom.v7i2.574

Tena S, Pella S.I, Mooy B.J. (2019). Implementasi Algoritma Rivest Code 6 (rc6) dan Steganografi Least Significant Bit (lsb) untuk keamanan data citra digital. *Jurnal Media Elektro*. Vol.08, No.02. Okt 2019. ISSN: 2252-6692