Jurnal Tera **E-ISSN : 2776-9666**
Volume 1, Issue 2, September 2021 **P-ISSN : 2776-1789**
Page 241-252

RANCANG BANGUN APLIKASI ENKRIPSI-DEKRIPSI SMS PADA ANDROID DENGAN METODE RC6

Kenneth Mohammad Albany Hakim[1]
[1] Jurusan Teknik Informatika, Fakultas Teknik dan Informatika, Universitas Dian Nusantara, Jakarta

Corresponding author
E-mail: kenneth.mohammad.albany.hakim@undira.ac.id

Diterima : 15/03/2021
Direvisi : 25/04/2021
Dipublikasi : 19/05/2021

Abstrak: Penerapan kriptografi dengan cara penyandian pesan merupakan salah satu solusi yang dapat digunakan untuk memenuhi aspek kerahasiaan. Pesan yang dikirim tersebut hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut menggunakan kunci rahasia. Perangkat yang digunakan dalam mengimplementasikan aplikasi SMS menggunakan platform yang berbasis android. Hal ini dikarenakan semakin maraknya ponsel yang berbasis android sampai sekarang.

Kata Kunci: Kriptografi, Android, Algoritma

PENDAHULUAN

SMS (Short Message Service) mungkin sudah tidak asing lagi dimata masyarakat, banyak sekali orang menggunakan fitur SMS untuk berinteraksi dengan orang serta alternative lain jika selular orang yang ingin dituju dalam keadaan off dan saat orang mengaktifkan selular mereka aka nada notifikasi pesan yang masuk. Banyak yang telah menggunakan fitur SMS dalam kehidupan sehari-hari, tetapi seiring berkembangnya waktu proses keamanan dalam melakukan pengiriman data pun semakin rawan yang dikarenakan banyaknya pihak ketiga yang dapat juga disebut sebagai hacker. Fitur layanan SMS saat ini belum memiliki standar keamanan yang baik, salah satu permasalahan yang muncul yaitu dari sisi human error dimana terjadi kesalahan penulisan nomor tujuan. Hal-hal tersebut menyebabkan kurang terjaminnya kerahasiaan pesan pengirim.

Penerapan kriptografi dengan cara penyandian pesan merupakan salah satu solusi yang dapat digunakan untuk memenuhi aspek kerahasiaan. Pesan yang dikirim tersebut hanya dapat dibaca oleh penerima yang memiliki hak untuk mengetahui isi pesan tersebut menggunakan kunci rahasia. Perangkat yang digunakan dalam mengimplementasikan aplikasi SMS menggunakan platform yang berbasis android. Hal ini dikarenakan semakin maraknya ponsel yang berbasis android sampai sekarang. Rumusan masalah yang di bahas dalam tugas akhir ini adalah :

Bagaimana cara membuat aplikasi SMS enkripsi-dekripsi menggunakan metode RC6 pada platform yang berbasis android?

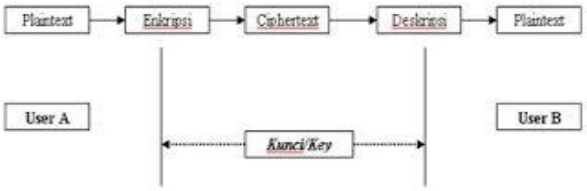
KAJIAN PUSTAKA

Kriptografi

Kriptografi berasal dari kata Yunani, yaitu Crypto yang berarti rahasia dan Grapho yang berarti menulis. Menurut (Scheiner , 1996) secara umum Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Cryptography is the art and science of keeping message secure). Menurut (Menezes , 1996) sebagai pembanding terdapat pula definisi yang berbeda, Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Algoritma kriptografi yang baik tidak ditentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Yang penting algoritma tersebut memiliki 4 persyaratan berikut :

1) Kerahasiaan pesan (plaintext) hanya dapat dibaca oleh dua pihak kewenangan.
2) Autentifikasi. Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain.
3) Integritas. Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi ketika dalam melakukan proses transmisi data.
4) *Non – Repudiation.* Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirim.

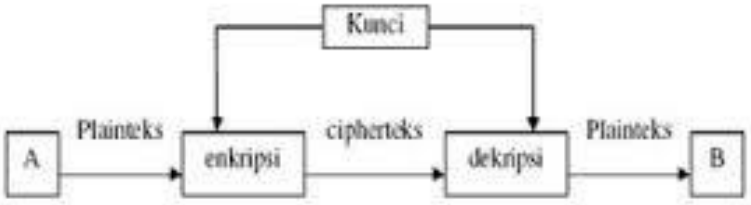
Menurut (Rhee , 1994) secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut :



Gambar 1. proses enkripsi dan dekripsi

Kriptografi Kunci Rahasia

Kriptografi kunci rahasia atau *secret key* adalah kriptografi yang hanya melibatkan satu kunci dalam satu proses enkripsi dan dekripsi. Proses dekripsi dalam kriptografi *secret key* ini kebalikan dari proses enkripsi

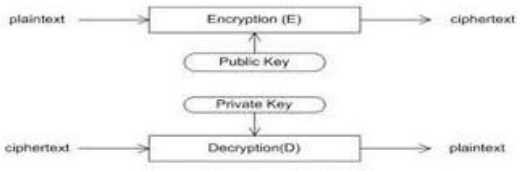


Gambar 2. Kriptografi Simetris

Kriptografi simetris dapat dibagi menjadi dua, yaitu penyandian blok *(block cipher)* dan penyandian alir *(stream cipher)*.

Kriptografi Kunci Publik

Kriptografi *public key* sering disebut dengan kriptografi asimetris. Berbeda dengan kriptografi *secret key*, kunci yang digunakan pada proses enkripsi dan proses dekripsi pada kriptografi *public key* ini berbeda satu sama lain. Jadi dalam kriptografi *public key*, suatu *key generator* akan menghasilkan dua kunci berbeda dimana satu kunci digunakan untuk melakukan proses enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi.



Gambar 3. kriptografi asimetris

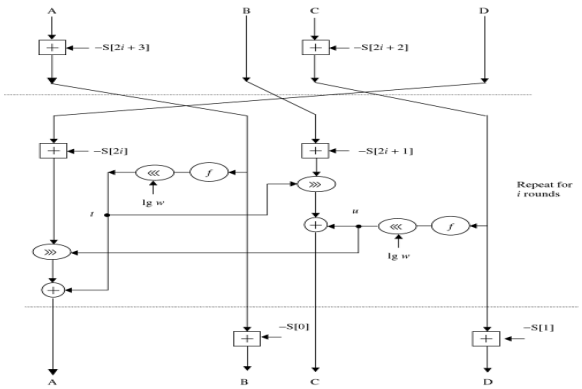
Kunci yang digunakan untuk melakukan enkripsi akan dipublikasikan kepada umum untuk dipergunakan secara bebas. Oleh sebab itu, kunci yang digunakan untuk melakukan enkripsi disebut juga sebagai *public key*. Sedangkan kunci yang digunakan untuk melakukan dekripsi akan disimpan oleh pembuat kunci dan tidak akan dipublikasikan kepada umum. Kunci untuk melakukan dekripsi ini disebut *private key*.

RC6

RC6 merupakan algoritma yang merupakan keturunan dari RC5 yang juga merupakan kandidat AES *(Advanced Encryption Standard)*. RC6 dirancang oleh Ron Rivest, Matt Robshaw, Ray Sidney, dan Yiqun Lisa Yin dan pertama kali di publikasikan tahun 1998. Algoritma RC6 seperti juga RC5 merupakan algoritma *cipher* yang terparameterisasi. RC6 secara tepat ditulis sebagai

$$RC6 - w / r / b$$

Nilai parameter w, r, dan b menyatakan hal yang sama seperti yang ditunjukkan dalam algoritma RC5. Algoritma RC6 yang dipakai sebagai kandidat AES adalah RC6-32/20/b, yang berarti ukuran *word* 32 bit, jumlah *round* 20 kali, dengan panjang kunci b ditentukan pengguna.



Gambar 4. Diagram Enkripsi RC6

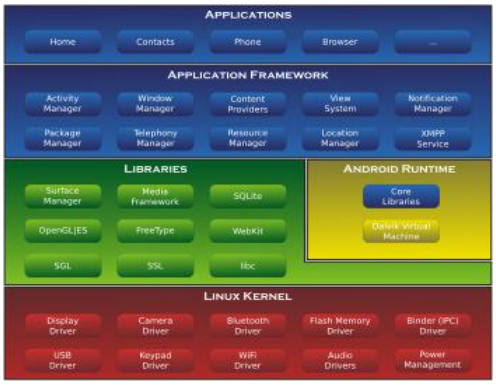
Keterangan :
A, B, C, D :Register
S[x] :Subkunci yang telah dibagi sebanyak 44 buah dari kunci

f	:Fungsi yang digunakan yaitu *f(x)=x(2x+1) (mod 2w)*
<<<	:pergeseran ke kiri sebanyak w kali
>>>	:pergeseran ke kanan sebanyak w kali
+	: proses penjumlahan
$\oplus$	: proses XOR
t	:hasil setelah diproses dengan fungsi
u	:hasil setelah diproses dengan fungsi
i	:putaran yang telah dilakukan

Android

Menurut (Android Developer, 2012) android adalah kumpulan perangkat lunak yang ditujukan bagi perangkat bergerak mencakup sistem operasi, *middleware*, dan aplikasi kunci. Android *Standart Development Kit* (SDK) menyediakan perlengkapan dan *Application Programming Interface* (API) yang diperlukan untuk mengembangkan aplikasi pada *platform* Android menggunakan bahasa pemrograman Java. Android dikembangan oleh Google bersama *Open Handset Alliance* (OHA) yaitu aliansi perangkat selular terbuka yang terdiri dari 47 perusahaan *Hardware, Software,* dan perusahaan telekomunikasi ditujukan untuk mengembangkan standar terbuka bagi perangkat selular.

Dalam paket sistem operasi Android terdiri dari beberapa unsur seperti tampak pada gambar 2.6. Secara sederhana arsitektur Android merupakan sebuah kernel Linux dan sekumpulan pustaka C / C++ dalam suatu *framework* yang menyediakan dan mengatur alur proses aplikasi.



Gambar 5. Arsitektur Android

SMS (Short Message Services)

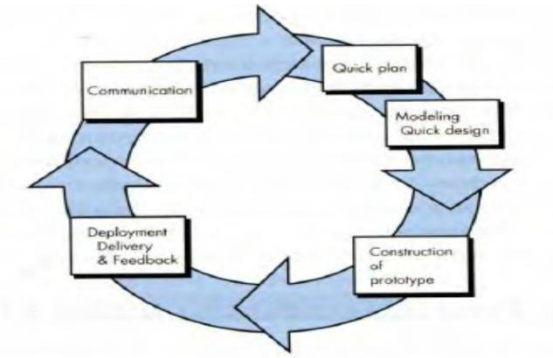
Menurut Rosidi (2004 : 1) *Short Message Service* (SMS) merupakan sebuah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukannya pengiriman pesan dalam bentuk *alphanumeric* antara terminal pelanggan dengan sitem eksternal seperti *email, paging, voice mail,* dan lain-lain. Mekanisme utama dalam sistem SMS yang dilakukan adalah melakukan pengiriman *short message* dari satu terminal pelanggan ke terminal yang lain. Hal ini berkat adanya sebuah entitas dalam Sistem SMS yang bernama *Short Message Service Center* (SMSC), disebut juga *Message Center* (MC). SMSC merupakan sebuah perangkat yang melakukan tugas *store and forward traffic short message.* Di dalamnya termasuk penentuan atau pencarian rute tujuan akhir dari *short message.*

Beberapa karakteristik SMS adalah:

a. Sebuah pesan terdiri atas 160 karakter yang mencangkup huruf atau angka. Juga dapat mendukung pesan *non-text* seperti format *binary*.
b. Prinsip kerjanya adalah menyimpan dan menyampaikan pesan *(store and forward message)*. Dengan kata lain, pesan tidak langsung dikirimkan ke penerima melainkan disimpan dahulu di *SMS – Centre.*
c. Memiliki ciri-ciri konfirmasi pengiriman pesan, yaitu pesan yang dikirimkan tidak secara sederhana dikirimkan dan dipercayai akan disampaikan dengan selamat, namun pengirim pesan dapat pula menerima pesan balik yang memberitahukan apakah pesan terkirim atau gagal.

Metode Pengembangan Prototype

Menurut (Pressman, 2005) dalam metode ini menerapkan sistem yang dimana saat pengguna menginginkan fitur-fitur dalam pembuatan perangkat lunak secara objektif, pengguna memerlukan gambaran dari proses *input*, proses, dan *output.* Di waktu yang sama pembuat perangkat lunak harus dapat memastikan algoritma apa yang lebih efisien dalam proses perangkat lunak dari segi perancangan *design*, sistem operasi yang akan digunakan dan evaluasi-evaluasi apa yang dapat membuat pengguna puas akan perangkat lunak ini. Untuk itu, dikondisi semacam ini, metode *prototype* merupakan metode yang cocok dalam masalah ini. *Prototype* dapat membuat pengguna untuk mengeri proses dari pengerjaan perangkat lunak serta tahap-tahap yang jelas. Tahap dari proses *prototype* ini dapat dilihat di gambar yang terdapat di bawah ini, yaitu :



Gambar 6. Tahap Metode *Prototype*

Dalam gambar yang terdapat pada 2.7, tahap awal dari metode ini adalah *communication* yang dimana pembuat perangkat lunak dan pengguna bertemu tatap muka dan membicarakan proses secara keseluruhan proses yang akan dibuat dalam perangkat lunak secara objektif, melakukan pemahaman serta analisis dan apa saja yang harus ada dalam perangkat lunak. Dari tahap *communication*, pembuat perangkat lunak dengan cepat melakukan proses perencanaan dan tahap awal secara cepat dan tepat *(quick plan)* dan menggambarkan model dari proses *input/output* dalam bentuk rancangan gambar *(modeling quick design)*. *Modelling* yang dimaksudkan meliputi tampilan-tampilan dari perangkat lunak. Setelah langkah *modeling* selesai, maka memasuki tahap selanjutnya, yaitu *construction of prototype* atau dapat disebut sebagai proses pembuatan perangkat lunak tersebut dan tahap pengujian dari perangkat lunak tersebut. Untuk tahan pengujian *(deployment and feedback)*, dilakukan oleh pengguna yang dimana saat pengguna merasa terdapat/belum puas akan perangkat lunak maka akan kembalik ke tahap *communication*. Proses tahap dalam metode *prototype* bersifat berulang-ulang sampai pengguna puas dan mengerti bahwa proses *input* dan *output* pada perangkat lunak tersebut.

Metode *prototype* dapat disebut sebagai "sistem pertama" dari perkataan Brook yang merupakan proses perancangan yang ideal antara hubungan pengguna dan pembuat perangkat lunak. Pengguna dapat merasakan proses dari pengerjaan perangkat lunak dan pembuat perangkat lunak dengan cepat membangun perangkat lunak.
Masalah yang terjadi saat metode *prototype* ini adalah :

1) Management software development yang tergolong kurang, dikarenakan saat pengguna menemukan adanya sistem yang tidak sesuai dengan kualitas pengguna, maka pembuat perangkat lunak harus membangun ulang sistem yang dianggap kurang oleh pengguna dan akan lebih banyak aktifitas "*maintenance*" disbanding jalannya proses sistem.
2) Pembuat perangkat lunak terkadang membuat perangkat lunak sesuai dengan rancangan *modeling* dan dengan bahasa pemrograman dan operasi sistem yang digunakan dengan sederhana, sehingga membuat pembuat perangkat lunak merasa nyaman akan proses itu dan lupa akan mengapa mereka dipilih oleh pengguna dalam pembuatan perangkat lunak.
3) Meski masalah ini dapat teratasi, *prototype* merupakan metode yang efisien dari perancangan sistem perangkat lunak. Salah satu kunci dalam metode ini adalah pengguna dan pembuat perangkat lunak harus setuju dan memiliki pemikiran yang sama dalam proses sistem ini.

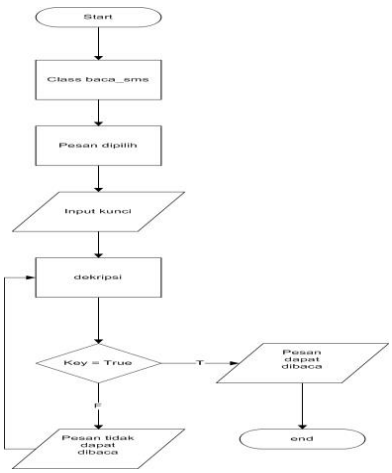
METODE PENELITIAN

Metode penelitian yang akan dilakukan adalah :

1) Mencari dan mereview beberapa jurnal dan previous research yang berhubungan dengan penelitian.
2) Mencari data kode karakter.
3) Membuat algortima enkriptor.
4) Membuat algortima deskriptor .
5) Konversi atau pengkodean algoritma menjadi program menggunakan perangkat lunak A.
6) Uji coba aplikasi dan dokumentasi.

HASIL DAN PEMBAHASAN

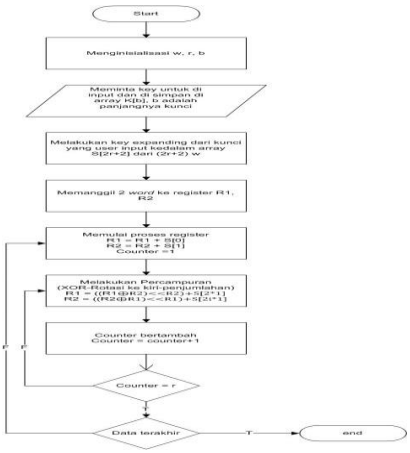
Perancangan Flowchart Baca Pesan



Gambar 7. Flowchart Baca Pesan

Ketika user memilih menu "Baca Pesan", maka akan dilakukan proses dari class baca_sms. Pesan yang sudah dipilih oleh user akan ditampilkan untuk kemudian diminta untuk memasukkan kunci yang sama pada saat proses enkripsi. Apabila kunci yang dimasukkan salah maka pesan tersebut tidak dapat dibaca. Namun, jika kunci yang dimasukkan benar, maka akan ditampilkan hasil pesan yang telah didekripsi sehingga user dapat membaca pesan tersebut.

Perancangan Flowchart RC6

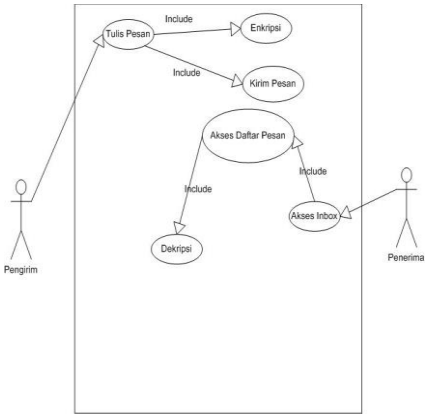


Gambar 8. Flowchart Metode RC6 Dalam Aplikasi SMS Kriptografi

Proses pertama yang dilakukan yaitu menginisialisasikan w, r, dan b dimana w=32, r =20, dan b=sesuai dengan input dari user. Setelah melakukan inisialisasi, dilanjutkan dengan meminta kunci yang akan dibagi menjadi 44 buah sub kunci dan disimpan pada array K[b]. Selanjutnya dilakukan pembangkitan kunci dari kunci yang telah diinput oleh user kedalam array S[2r+2] dari (2r+2)w. Setelah membangkitkan kunci, dilakukan pemanggilan 2 w(*word*) ke dalam register R1, dan R2. Proses register dimulai dengan counter yang diawali dari 1. Selanjutnya melakukan proses pencampuran, yaitu XOR, pergeseran ke kiri, dan penjumlahan. Setelah proses pencampuran selesai nilai counter ditambah 1. Saat nilai counter bertambah inilah sudah dilakukan 1 kali iterasi yang dilakukan terus menerus hingga nilai counter = r yaitu 20.

Perancangan Use Case

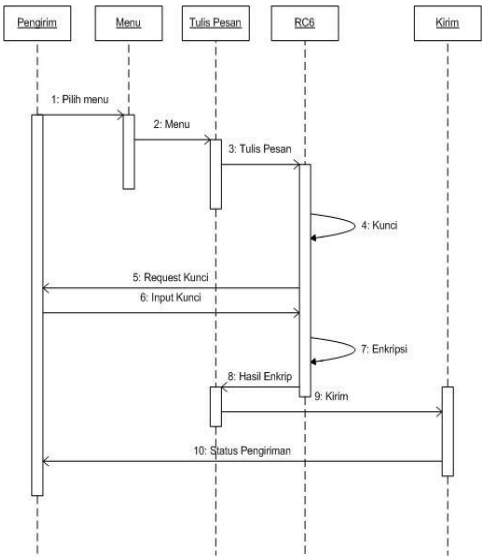
Berikut adalah Use Case dari aplikasi ini :



Gambar 9. Use Case Diagram Aplikasi

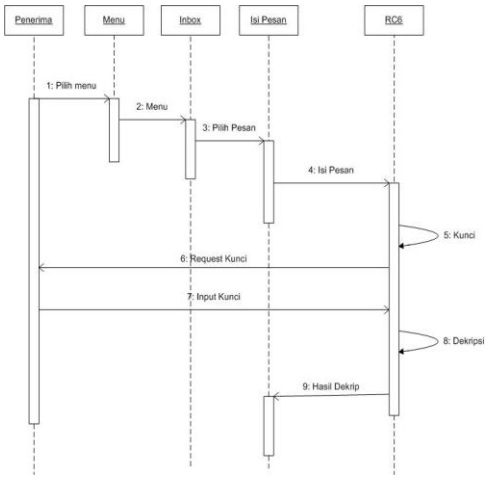
Keterangan :
1) Menggunakan 2 aktor, yaitu Pengirim dan Penerima.
2) Pengirim dapat mengakses Tulis Pesan yang didalamnya sudah termasuk proses enkripsi dan kirim pesan.
3) Penerima dapat mengakses inbox untuk yang didalamnya sudah termasuk proses akses ke daftar pesan dan dekripsi.

Perancangan Sequence



Gambar 10. Sequence Diagram Tulis Pesan

Pengirim memilih Menu, dalam hal ini yaitu tulis pesan. Setelah memilih tulis pesan, pengirim diminta untuk memasukkan kunci yang kemudian kunci tersebut diproses pada class RC6. Setelah memasukkan kunci, proses enkripsi dilakukan pada class RC6. Hasil enkripsi dari pesan kemudian ditampilkan pada tulis pesan sehingga pengirim dapat melihat pesan yang telah dienkripsi. Kemudian pengirim melakukan kirim pesan yang jika pesan telah terkirim akan muncul status pengiriman.

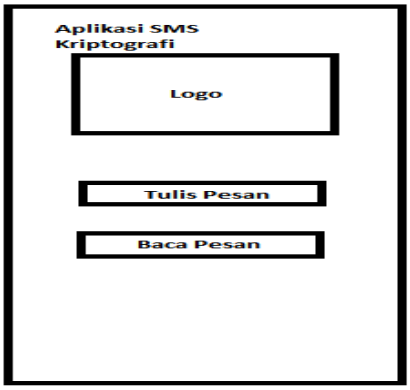


Gambar 11. Sequence Diagram Baca Pesan

Penerima pesan memilih menu baca pesan, yang dapat diakses melalui class inbox. Setelah pesan dipilih maka penerima akan diminta untuk memasukkan kunci yang sama dengan pengirim. Kunci yang sudah diinput kemudian dilanjutkan dengan proses dekripsi yang terjadi di class RC6. Setelah hasil dekripsi didapat, hasil tersebut akan ditujunkan kepada penerima.

Perancangan Antarmuka

Proses tampilan rancangan dari aplikasi ini adalah :

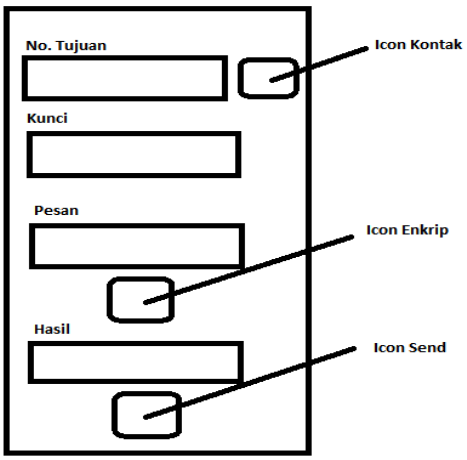


Gambar 12. Menu Awal Aplikasi

Keterangan :

1. Logo:Gambar logo dari aplikasi ini
2. Tulis Pesan:Menu untuk mengirimkan pesan
3. Baca Pesan: Menu untuk membaca pesan

Aplikasi ini sengaja dirancang semudah mungkin, agar user tidak mendapati kesulitan saat menggunakan aplikasi. Berikut adalah rancangan tampilan dari menu “Tulis Pesan” :



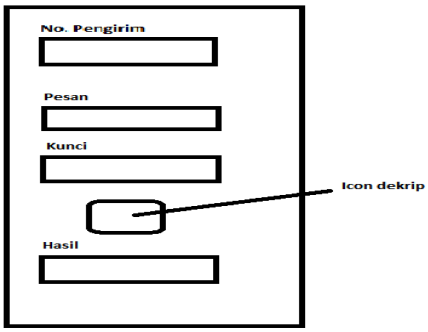
Gambar 13. Tampilan Tulis Pesan

Keterangan :

1. No. Tujuan : diisi dengan nomor tujuan
2. Kunci : kunci yang diinput oleh user
3. Pesan : isi pesan yang akan dikirimkan
4. Hasil : tampilan dari pesan yang sudah di enkripsi
5. Icon Kontak : button untuk mengambil kontak dari buku telepon
6. Icon Enkrip : button untuk melakukan proses enkripsi

7. Icon Send : button untuk mengirimkan hasil enkripsi

Berikut adalah rancangan tampilan dari menu “Baca Pesan” :



Gambar 14. Tampilan Baca SMS

Keterangan :
1. No. Pengirim : berisi keterangan nomor pengirim pesan
2. Pesan : pesan yang telah dikirimkan
3. Kunci : kunci yang diinput oleh user
4. Hasil : hasil dari pesan yang telah didekripsi
5. Icon Dekrip : button yang digunakan untuk melakukan dekripsi

Rancangan ini dibuat seminimal mungkin agar dapat mempermudah user dalam penggunaan aplikasi.

Implementasi

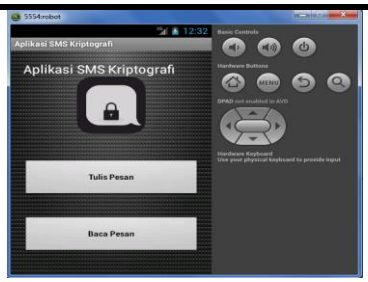
Setelah melakukan analisa dan perancangan aplikasi, langkah selanjutnya adalah pengkodean *(*implementasi) dan pengujian. implementasi merupakan desain (perancangan) aplikasi dengan kode-kode tertentu yang dapat dimengerti oleh mesin dengan *spesifikasi* perangkat lunak (*software*) dan perangkat keras (*hardware*) yang digunakan.

Spesifikasi Perangkat Lunak

Spesifikasi perangkat lunak yang dipakai dalam proses pembuatan aplikasi :
1. Microsoft Windows 7 Ultimate 64Bit
2. Eclipse Juno Version: 1.4.1.v20120912
3. Android Developer Tools (ADT)
4. Java Development Kit (Versi 8)
5. Android SDK

Pengujian Aplikasi

Tahap pengujian ini dilakukan menggunakan emulator android pada android SDK.
Contoh :
Pengguna 1 dengan nomor telepon 5554 ingin mengirimkan pesan rahasia ke pengguna 2 dengan nomor telepon 5556. Berikut tahap implementasi dari aplikasi ini :
Pengguna 1 membuka aplikasi lalu memilih menu “Tulis Pesan”.

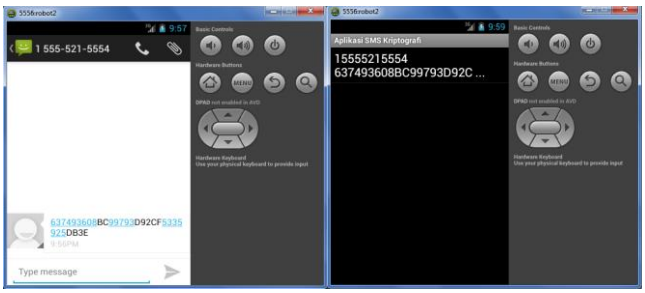


Gambar 15. Membuka Aplikasi SMS

Ketik no tujuan pengguna 2 (5556), isi pesan ("Selamat pagi"), isi kunci (654321), klik gambar kunci untuk menyandikan pesan yang sudah di isi, hasil dari pesan yang sudah di sandikan akan muncul, dan klik gambar kirim pesan untuk mengirimkan pesan.

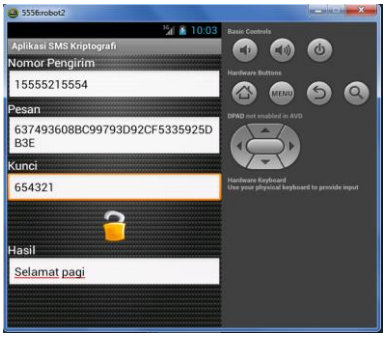
Gambar 16. Proses Mengirimkan SMS

Dapat dilihat bahwa pesan yang dikirim adalah ("Selamat pagi") Pengguna 2 akan menerima pesan dari pengguna 1 dalam 2 sisi yaitu:



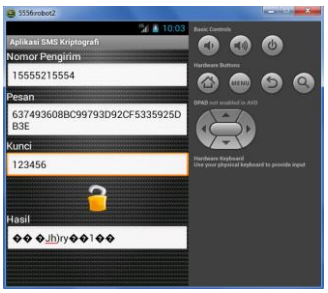
Gambar 17. Tampilan Inbox Dari Dua Sisi

Sisi pertama ditampilkan di list inbox bawaan android dan sisi kedua adalah list pesan yang ditampilkan di inbox pada aplikasi. Pengguna 2 melalukan klik pada pesan yang ingin di dekripsikan. Pengguna 2 diharuskan mengisi kunci yang sama dengan pengguna 1.



Gambar 18. Proses Dekripsi Pesan

Jika kunci yang diinputkan benar maka pesan asli dapat muncul pada textfield hasil. Jika kunci yang diinputkan salah, maka akan menghasilkan



Gambar 19. Proses Dekripsi Pesan Dengan Kunci Yang Salah

Pesan yang tampil adalah simbol yang tidak dapat dibaca oleh manusia.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil dari pembuatan aplikasi SMS Kriptografi dengan menerapkan metode RC6 pada android, maka didapatkan kesimpulan seperti berikut:

1) Dengan aplikasi ini, dapat memudahkan dalam melakukan proses pengiriman dan penerimaan pesan yang bersifat sangat penting dan rahasia.
2) Membuktikan bahwa metode RC6 dapat diterapkan untuk proses pengiriman pesan dan penerimaan pesan berbasis SMS.

Saran

Saran-saran yang diberikan untuk aplikasi ini adalah :

1) Aplikasi ini hanya digunakan sebatas mengirimkan pesan berupa *text* tanpa menyisipkan gambar ataupun suara.
2) Proses pengiriman kunci dilakukan di luar aplikasi.
3) Hanya menggunakan 1 kunci dikarenakan menerapkan metode RC6.

DAFTAR RUJUKAN

Bruce Schneier, *Applied Cryptography:Protocols,Algorithms, and Source Code in C*, USA, John Wiley & Sons, Inc., 1996.

Menezes, A. dkk, "*Handbook of Applied Cryptography"*, CRC Press, Inc., 1996.

Munir, Rinaldi. Bahan Kuliah IF5054 Kriptografi. (2004). Departemen Teknik Informatika, Institut Teknologi Bandung.

Rhee, Man Young. *Cryptography and Secure Communications,* Singapore, McGraw-Hill Book Co., 1994.

Roger S Pressman, "*Software Engineering Sixth Edition",* USA, McGraw-Hill, 2005.

Rosidi, R, I. 2004. *Membuat Sendiri SMS Gateway (ESME) Berbasis Protokol SMPP*. Yogyakarta : ANDI

Sayed Y. Hashimi and Satya Komantineni, 2009. *Pro Android*, Apress Inc.