RANCANG BANGUN APLIKASI SHORT MESSAGE SERVICE (SMS) MENGGUNAKAN ALGORITMA RSA-RC6 BERBASIS ANDROID

Azis Ihyaulumiddin[1], Zulfan Khairil Simbolon[2], Muhammad Rizka[3]

[1,3] *Jurusan Teknologi Informasi dan Komputer Politeknik Negeri Lhokseumawe*
Jln. B.Aceh Medan Km.280 Buketrata 24301 INDONESIA

[1]azis@gmail.com
[1]zulfan@pnl.ac.id
[3]muhammad.rizka910@gmail.com

***Abstrak*— Perkembangan teknologi berkembang sangat cepat. Hal ini dapat dilihat dari bermunculan ponsel pintar dengan berbagai fitur dan memiliki sistem operasi kompleks layaknya komputer. Berbagai sistem operasi untuk ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Ponsel pintar yang memiliki berbagai fitur, salah satu fitur yang disediakan adalah pesan singkat (*Short Mesagge Service*). Fitur SMS yang disediakan memiliki kerentanan terhadap keamanan informasi data. Dengan melakukan enkripsi terhadap teks SMS maka tingkat keamanan informasi dari pesan dapat ditingkatkan. Metode kriptografi dapat diimplementasikan pada SMS untuk meningkatkan keamanan informasi data. Metode kriptografi yang diimplementasikan pada penelitian ini adalah RSA-RC6 (Rivest Shamir Adleman-Rivest Code 6). Dengan menggunkan metode RSA-RC6 pada plainteks dengan panjang 13 karakter sampai 100 karakter hanya membutuhkan waktu enkripsi rata-rata 0,0023 detik dan proses dekripsi rata-rata 0,0030 detik. Penilitian ini bertujuan untuk mengamankan isi pesan sms yang sangat mudah untuk di akses oleh pihak tertentu, dan bermanfaat bagi mereka yang ingin mengamankan sms yang sangat rahasia.**

Kata kunci : Android, SMS, Enkripsi, Dekripsi, RSA-RC6, Waktu.

Abstract*— *The development of technology is developing very fast . It can be seen from popping smart phones with different features and has a complex operating system like a computer. Variety of operating systems for mobile phones also appear, including a fairly well known is android. Smart phone that has a variety of features, one of the features provided are short messages(Short Mesagge Service). SMS features are provided vulnerability to information security data. By encrypting the SMS text message level of information security can be improved. Cryptographic methods can be implemented in the SMS to improve information security data. Cryptographic methods implemented in this study is the RSA-RC6 (Rivest Shamir Adleman-Chines Reminder Theorem). By using RSA-RC6 method in plaintext with a length of 13 characters to 100 characters only takes an average of encryption and decryption process 0.0023 seconds on average 0.0030 seconds. This research aims to secure the contents of SMS messages is very easy to access by certain parties, and useful for those who want to secure sms highly confidential

Keyword : *Android, SMS, Encryption, Decryption, RSA-RC6, Time.*

I. PENDAHULUAN

Perkembangan teknologi saat ini sangat pesat dan diikuti dengan kebutuhan manusia untuk mendapatkan fasilitas-fasilitas yang dapat mendukung upaya penyelesaian pekerjaan. Penggunaan teknologi telepon genggam (*handphone*) sebagai alat telekomunikasi pada saat ini telah mengubah cara pandang masyarakat dalam berkomunikasi. Keamanan data merupakan sesuatu yang harus diperhatikan dalam kemajuan teknologi informasi, terutama dalam pesan yang berbentuk teks. Sistem keamanan pesan yang berbentuk teks salah satunya dengan sistem kriptografi. Sistem kriptografi adalah ilmu yang menggunakan teknik

matematika sebagai landasan untuk membuat sebuah Aplikasi keamanan informasi. Tujuan utama Aplikasi kriptografi adalah mengamankan informasi yang bersifat rahasia serta menjaga keutuhan informasi tersebut. Salah satunya adalah menjaga kemanan terhadap pesan yang berbentuk teks. Salah satu metode kriptografi adalah metode RSA (Rivest, Shamir, Adleman) – RC6 (Rivest Code 6). Dalam hal ini RSA – RC6 menggunakan dua metode untuk keamanan sms, RSA digunakan untuk proses pembangkit kunci dan RC6 digunakan untuk proses keamanan pengiriman kunci RSA.

II. METODOLOGI PENELITIAN

Metode yang digunakan pada penelitian ini adalah RSA dengan RC6 adalah sistem kriptografi yang dimodifikasi untuk membuat sebuah aplikasi enkripsi. RC6 dalam RSA bertujuan untuk keamanan proses pengiriman kunci, sehingga dengan menggunakan RC6 proses pengiriman kunci dan sms akan lebih aman.

2.1 Pembangkit kunci RSA – RC6

Pada pembangkit kunci RSA – RC6 eksponen dekripsi n tidak secara langsung diberikan pada kunci private namun dapat dihitung melalui parameter dP, dQ, dan qInv yang memiliki ukuran setengah dari panjangn bit n. Algoritma pembangkit kunci RSA – RC6 adalah sebagai berikut :

1. Pilih dua buah bilangan prima sembarang, p dan q

2. Hitung n = p . q (sebaiknya p ≠ q , sebab jika p = q maka n = p! sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n)

3. Hitung ω n = (p − 1)(q − 1)

4. Pilih e, yang relatif prima terhadap ω (n)

5. d = e-1 pada ω (n)

6. dP = d mod p − 1

7. dQ = d mod (q − 1)

8. qInv = q-1 pada p

9. Kpublic =(e, n) , Kprivat = (dP, dQ, qInv, p, q).

2.2 Enkripsi RSA – RC6

Dalam proses enkripsi RSA – RC6 tidak mengalami perbedaan dengan enkripsi pada algoritma RSA biasa dengan menggunakan fungsi :

$$Ci = Mi^{e} \bmod n \quad (2.1)$$

Dimana:
Ci = *chipertext*
Mi = *plaintext*
e,n = kunci publik

2.3 Dekripsi RSA – RC6

Dalam proses dekripsi RSA – RC6 dengan menghitung kembali d dengan menggunakan parameter pada kunci privat, yaitu dP, dQ, dan qInv. Berdasarkan penyelesaian persoalan CRT d dapat dihitung kembali sehingga memulihkan teks sandi untuk mendapatkan kembali teks asli. Fungsi yang digunakan untuk mendekripsi teks sandi adalah sebagai berikut :

1. $M_1 = Ci^{dP} \bmod p$ (2.2)
2. $M_2 = Ci^{dQ} \bmod q$ (2.3)
3. $h = qInv.(M_1-M_2) \bmod p$ (2.4)
4. $M_i = m_2 + h.q$ (2.5)

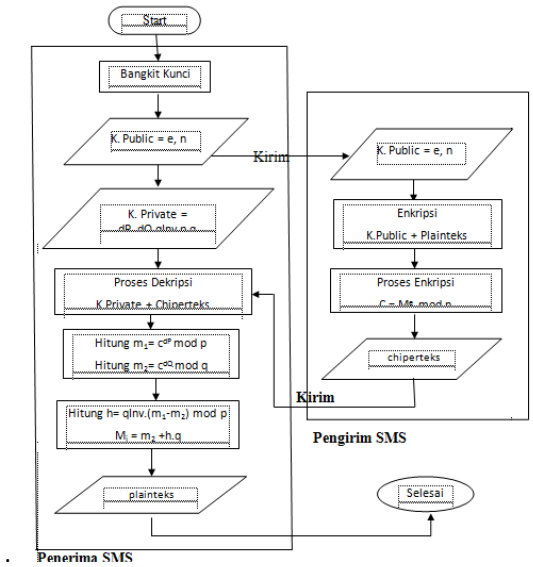
Dimana:
Mi = *plaintext*
Ci = chipertext
dP, dQ, p,q dan qInv = kunci privat

2.4 Android

Android adalah sebuah sistem operasi mobile yang berbasiskan pada versi modifikasi dari linux. Pertama kali sistem operasi ini dikembangkan oleh perusahaan Android.Inc. Google mengakuisisi perusahaan Android Inc. pada tanggal 17 Agustus 2005 dan menjadikannya sebagai anak perusahaan yang dimiliki oleh Google. Pendiri Android Inc. yaitu Rubin, Miner, serta White tetap bekerja pada perusahaan tersebut setelah diakuisisi oleh Google. Di Google, tim yang dipimpin oleh Andy Rubin mulai untuk mengembangkan sebuah platform perangkat seluler dengan menggunakankernelLinux.Sejak tahun 2008, Android mulai secara bertahap melakukan sejumlah pembaruan atau update untuk meningkatkan kinerja dari sistem operasi tersebut dengan menambahkan fitur baru, memperbaiki bug pada versi android yang sebelumnya. Setiap versi yang dirilis dinamakan secara alfabetis dengan berdasarkan nama sebuah makanan pencuci mulut, seperti cupcake, donut, dan sebagainya (Febrian, 2014)

2.5 Flowchart Proses Kerja Aplikasi

Pada gambar 1 berikut menunjukkan Flowchart keseluruhan proses aplikasi kriptografi menggunakan algoritma *RSA-RC6*. Proses kerja sistem ini diawali dengan user memulai aplikasi kemudian sistem menampilkan pilihan menu yang tersedia didalam aplikasi kriptografi SMS, jika user memilih salah satu menu maka user akan masuk ke menu pilihan tersebut, akan tetapi apabila user tidak memilih salah satu menu tersebut maka sistem akan berhenti.



III. HASIL DAN PEMBAHASAN

3. Hasil dan Pembahasan :

Hasil pengujian sistem enkripsi dan dekripsi mudah dimengerti oleh user dengan baik. Hasil pengujian aplikasi sms RSA-RC6 adalah sebagi berikut:

3.1 Tampilan Menu Utama

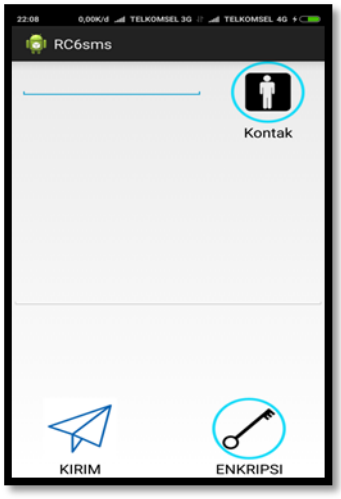
Pada tampilan menu utama aplikasi sms enkripsi dan dekripsi ini terdiri dari tombol menu Tulis Pesan, Pesan Masuk, Pembangkit Kunci, Bantuan, Pesan Keluar dan Tentang. Setiap pilihan tombol menu yang terdapat pada menu utama memiliki fungsi dan activity masing-masing. Pemanggilan pada menu ini menggunakn method setOnClickListener(). Berikut adalah salah satu contoh program pada menu utama pada aplikasi ini dapat dilihat pada Gambar 1 berikut :

Gambar 1 Form Meu Utama

Gambar 1 memperlihatkan hasil tampilan *form* utama yang berisi menu-menu utama sistem sesuai dengan perancangan yaitu menu tulis pesan, pesan masuk, pembangkit kunci, bantuan, pesan keluar dan tentang.

3.2 Tampilan Menu Tulis Pesan

Pada menu ini adalah tempat menyandikan pesan yang berbentuk planteks menjadi chiperteks dan kemudian dikirimkan ke penerima. Adapun tampilan form tulis pesan adalah sebagai berikut :

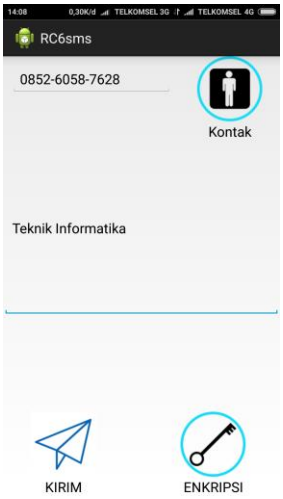


Gambar 2. Form Tulis Pesan

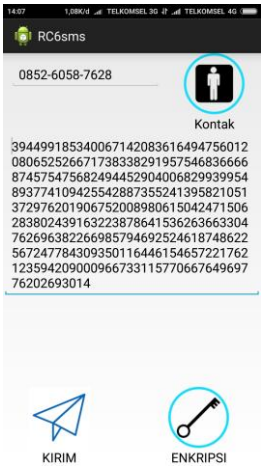
Pada menu Tulis Pesan seperti yang terlihat pada gambar 2 terdapat objek EditTeks yang pertama untuk

mengisi nomor tujuan, dan di sampingnya terdapat button kontak untuk menginput nomor dan di bawah ada EditText untuk mengisi pesan, dan di bawah ada button kirim dan button enkripsi. enkripsi yaitu untuk mengenkripsi pesan yang sudah di inputkan pada EditTeks pesan. Setelah di enkripsi maka akan keluar chipertext dan selanjutnya akan dikirimkan pesan yang sudah terenkripsi kepada penerima dengan menekan tombol kirim. Jika user ingin mengirimkan pesan yang tidak terenkripsi maka user dapat memasukkan pesan langsung pada EditTeks chiper maka dengan menekan tombol kirim juga pesan akan terkirim ke penerima.

Gambar 3 dan Gambar 4 akan memperlihatkan bagaimana proses enkripsi terjadi pada form Tulis Pesan.



Gambar 3 pesan sebelum di enkripsi



Gambar 4 pesan telah di enkripsi

Setelah pesan di enkripsi maka pesan akan dikirim ke penerima untuk di dekripsi.

3.3 Tampilan Menu Pesan Masuk :

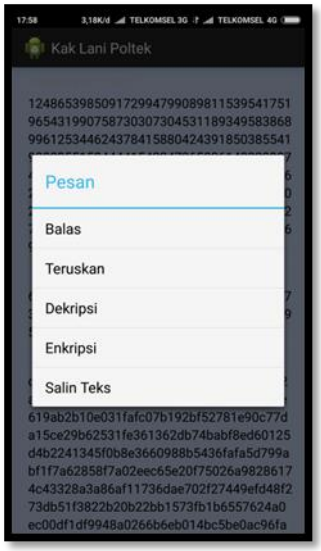
Pada menu ini adalah tempat untuk melihat pesan yang sudah dikirim oleh user. Dan tempat untuk mendekripsikan pesan yang berupa ciphertext. Adapun tampilan form tulis pesan adalah sebagai berikut.

Gambar 5 tampilan menu pesan masuk

Adapun pada menu ini adalah tempat sms masuk, apabila user ingin membaca sms tersebut user hanya perlu menekan salah satu pesan yang ingin dibaca. Setalah pesan ditekan maka akan muncul form kotak masuk detail sekaligus untuk mendekripsikannya. Adapun tampilan form adalah sebagai berikut :

Gambar 6 sms yang akan di dekripsi

Gambar 7 isi sms terenkripsi

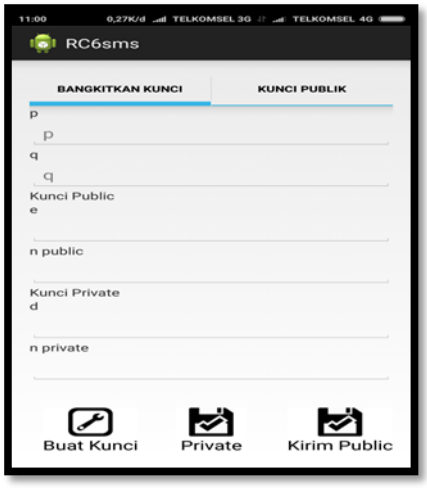


Gambar 8 sub sms pesan masuk

Gambar 9 pesan berhasil di dekripsi

Pada menu Pesan Masuk seperti yang terlihat pada gambar 5 s/d gambar 9 proses dekripsi menggunakan kunci private yang telah di simpan di dalam database, perintah untuk memanggil kunci private yang ada di dalam database Cursor cursor = db.rawQuery("SELECT * FROM kuncipriva te ",**null**); Makan pesan akan secara automatis terdekripsi tanpa memasukan kunci dekripsi secara manual.

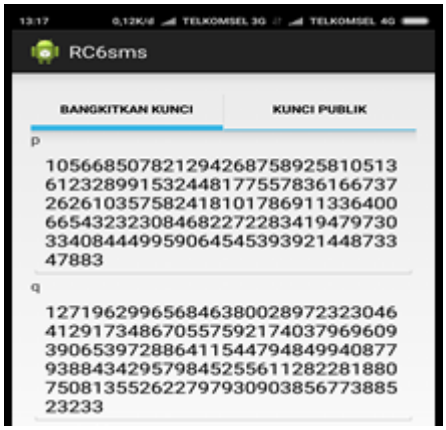
3.4 Tampilan Menu Pembangkit Kunci



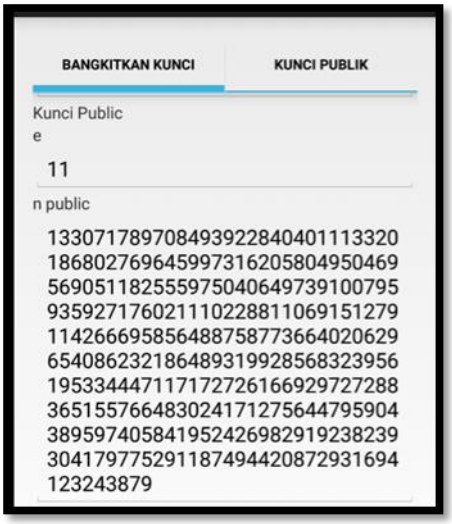
Gambar 10 tampilan pembangkit kunci

Pada menu pembangkit kunci terdapat tombol buat kunci private, kirim public seperti terlihat pada gambar 10 ketika tombol buat kunci di tekan maka akan membangkitkan

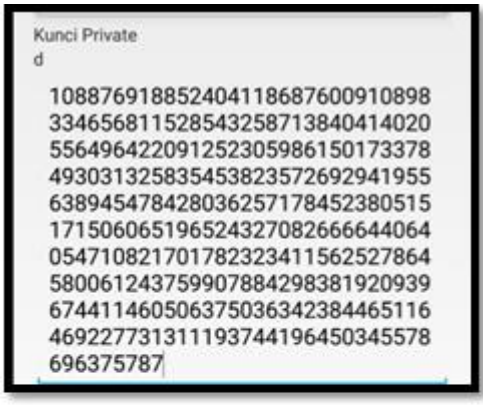
nilai objek EditTeks pada form tersebut. EditTeks pada form pembangkit kunci adalah untuk memperoleh nilai p, nilai q$\varphi(n)$, kunci public e,n dan kunci private dp, dq, qInvs, p dan q. maka jika tombol buat kunci di klik akan tampil tampilan seperti gambar 11 s/d gambar 13 sebagai berikut :

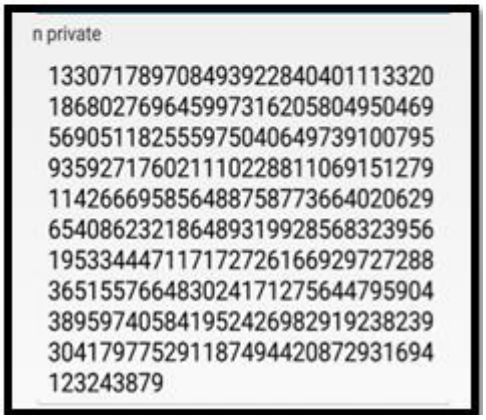


Gambar 11 proses pembangkit kunci



Gambar 12 kunci public





Gambar 13 kunci private

Perintah diatas akan dijalankan ketika user menekan tombol buat kunci. Sistem akan mengacak bilangan prima p dan q dengan panjang bilangan prima tersebut 512 bit perintah acak bilangan tersebut adalah

```
Random r = new SecureRandom();
BigInteger p = BigInteger.probablePrime(512, r);
BigInteger q = BigInteger.probablePrime(512, r);
```

Setelah p dan q yang diacak dapat maka sistem akan menampilkan di form, selanjutnya sistem akan mencari nilai n, nilai pn, nilai e, nilai d, nilai dP, niali dQ, nilai qInvs. Pada metode RSA-RC6 berbeda dengan metode RSA dimana pada metode ini menggunakn nilai p dan nilai q untuk kunci private.

3.5 Tampilan Menu Bantuan

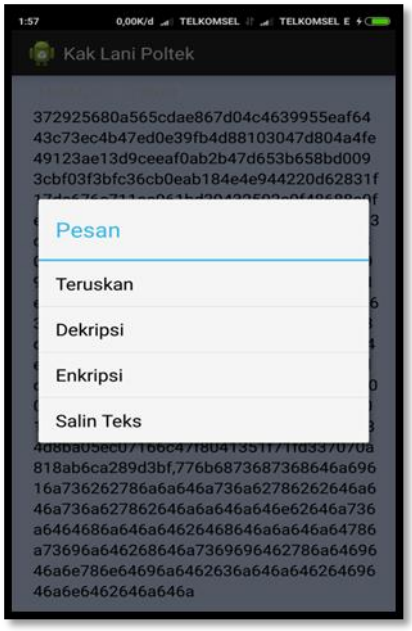
Pada menu ini akan ditampilkan informasi mengenai Menu Utama (*Activity_Main*) yaitu Tulis Pesan, Pesan Masuk, Pembangkit Kunci, Bantuan, Pesan Keluar, Tentang.

Gambar 14 tampilan menu bantuan

3.6 Tampilan Menu Pesan Keluar

Pada menu ini adalah tempat untuk melihat pesan yang sudah terkirim, dan memiliki beberapa sub menu seperti , Teruskan, Dekripsi, Enkripsi dan Salin Teks seperti gambar berikut ini :

Gambar 15 tampilan menu pesan keluar



Gambar 16 sub menu pesan keluar

Pada menu ini akan ditampilkan informasi mengenai profil tentang pembuat aplikasi. Adapun tampilan menu tentang dapat dilihat pada gambar 4.18 berikut.

Gambar 17 tampilan menu tentang

IV. KESIMPULAN

Setelah melakukan pengujian dan pembahasan mengenani perancangan sistem keamanan sms menggunakan algoritma RSA-RC6 dapat di ambil kesimpulan sebagai berikut :

1. Metode RSA dapat diimplementasikan pada proses enkripsi dan dekripsi pesan sms.
2. Metode RC6 dapat diimplementasikan pada proses pengiriman kunci.
3. Proses keamanan pengiriman kunci RSA dengan menggunakan RC6 sangat penting agar proses pengiriman kunci lancar dan aman.
4. Dengan menggunakan keamanan sms dengan metode RSA-RC6 maka pesan akan lebih aman dan terjaga.
5. Pada metode ini proses pengiriman kunci sedikit lama karena terlalu besar bit yang digunakan.
6. Waktu rata-rata proses enkripsi adalah 0.0122 detik. sedangkan pada proses dekripsi waktu yang dibutuhkan juga sangat berdekatan dan bahkan mempunyai kecepatan yang sama. Dari proses dekripsi dapat di peroleh nilai rata-rata proses dekripsi adalah 0.0293 detik.

V. REFERENSI

[1] FEBRIAN BUDI UTAMA, (2014)" APLIKASI SMS NGAN METODE RSA PADA SMARTPHONE ANDROID". HAL 1-20

[2] Hendri Syaputra dan Hendrik Hendrik Fery Herdiyatmoko, (2012) " Aplikasi Enkripsi Data Pada File Teks Dengan Algoritma RSA (*RIVEST SHAMIR ADLEMAN*)". Jurnal Teknologi Informasi & Komunikasi Terapan, hal 229-234

[3] Dafid, (2006) "Kriptografi Kunci Simetris Dengan Menggunakan Algoritma *Crypton"* , STMIK MDP Palembang, Volume 2 Nomor 3. Hal 20-27.

[4] Sitorus, S dkk. 2006. *Pengolahan Citra Digital.* Medan : USU.

[5] Hartini, Primaini S, (2014) "Kriptografi *Password* Menggunakan Modifikasi Metode Affine Ciphers *" ,* Amik Sigma, Palembang, Volume 2 Nomor 1. Hal 40-50.

[6] Hasugian, Abdul H, (2013) " Implementasi Algoritma Hill Cipher Dalam Penyandian Data *" ,* STMIK Budi Darma Medan, Volume 2 Nomor 4. Hal 115-122.

[7] Haviluddin, (2011) , Memahami Penggunaan UML (*Unified Modelling Language) " , FMIPA Universitas Mulawarman*, Volume 6 Nomor 1. Hal 1-15.

[8] A.S Rosa dan Salahuddin M, 2011. *Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek),* Modula, Bandung.