# RANCANG BANGUN APLIKASI ENKRIPSI SMS (SHORT MESSAGE SERVICE) DENGAN METODE RSA PADA TELEPON SELULAR BERBASIS ANDROID

**Isna Fauzia Rahmah [1], Banni Satria Andoko [2]**

Program Studi Teknik Informatika, Jurusan Teknologi Informasi, Politeknik Negeri Malang
JL. Soekarno-Hatta No. 9 Malang 65141, Indonesia
[1] isnafauziarahmah@gmail.com, [2] ando@polinema.ac.id

**Abstrak**

Semakin pesatnya perkembangan teknologi terutama pada pada teknologi yang berbasis mobile. Telepon selular ini menyediakan media komunikasi yang beragam, salah satunya adalah SMS (Short Message Service). Namun komunikasi via SMS ini memiliki celah keamanan, karena pesan yang dikirimkan akan disimpan di SMSC (Short Message Service Center), yaitu perantara pengirim, penerima, dan menyimpan SMS tersebut dalam waktu tertentu. Pesan yang sifatnya plaintext ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. SMS sendiri juga dapat melakukan roaming jaringan setempat hingga ke jaringan asing sehingga dimungkinkan SMS spoofing dalam bentuk penyamaran atau manipulasi informasi seperi alamat atau data lainnya yang menyerupai user pada umumnya. Akibatnya, informasi penting seperti password, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya, isi SMS yang dikirim juga terbuka di sistim penyedia jasa maupun pegawainya. Maka dibuatlah Enkripsi SMS untuk menyelesaikan masalah diatas.

Aplikasi Enkripsi SMS berguna menjadi sebuah alternatif solusi media pengiriman SMS secara aman. Aplikasi ini mampu mengirimkan pesan yang telah dienkripsi sekaligus mendekripsi pesan tersebut. Enkripsi SMS ini menggunakan metode RSA yang merupakan algoritma enkripsi maupun deskripsi dalam kriptografi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapa pun kecuali orang-orang yang berhak. Terbukti dari hasil pengujian yang dilakukan, metode RSA ini berjalan dengan baik untuk mengamankan SMS. Namun jumlah pesan pada SMS mengalami peningkatan jumlah karakter sehingga untuk memperkecil jumlah pesan terenkrip maka pesan dikembalikan dalam bentuk karakter. Jumlah pesan pada Aplikasi ini juga tidak bisa lebih besar dari n atau hasil dari p*q.

**Kata kunci**: Enkripsi, Dekripsi, SMS, RSA

## 1. Pendahuluan

Semakin pesatnya perkembangan teknologi terutama pada pada teknologi yang berbasis mobile. Salah satunya adalah telepon selular (ponsel) yang semakin banyak fitur dan aplikasi yang dapat digunakan untuk berbagai fungsi. Telepon selular ini menyediakan media komunikasi yang beragam, salah satunya adalah SMS (Short Message Service). SMS menjadi popular di kalangan masyarakat karena dengan begitu mudahnya kita dapat saling bertukar informasi tanpa batasan jarak dan waktu.

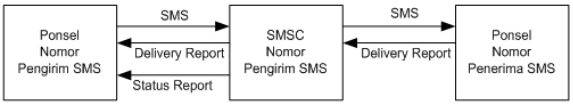
Namun komunikasi via SMS ini memiliki celah keamanan, karena pesan yang dikirimkan akan disimpan di SMSC (Short Message Service Center), yaitu perantara pengirim, penerima, dan menyimpan SMS tersebut dalam waktu tertentu. Pesan yang sifatnya plaintext ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. SMS sendiri juga dapat melakukan roaming jaringan setempat hingga ke jaringan asing sehingga dimungkinkan SMS spoofing dalam bentuk penyamaran atau manipulasi informasi seperi alamat atau data lainnya yang menyerupai user pada umumnya. Akibatnya, informasi penting seperti password, nomer pin, dan lain-lain dapat dibaca oleh orang yang tidak berhak untuk mengetahuinya, isi SMS yang dikirim juga terbuka di sistim penyedia jasa maupun pegawainya.

Oleh karena itu, penulis akan mencoba membuat sebuah aplikasi pengamanan sms dengan metode RSA untuk meningkatkan aspek confidentiality, integrity, authenticity dan nonrepudiation pada perangkat mobile berbasis Android. RSA yang menggunakan algoritma asimetrik mempunyai dua kunci yang berbeda, disebut pasangan kunci (key pair) untuk proses enkripsi dan dekripsi. Kunci-kunci yang ada pada pasangan kunci mempunyai hubungan secara matematis, tetapi tidak dapat dilihat secara komputasi untuk mendeduksi kunci yang satu ke pasangannya. Algoritma ini disebut kunci publik, karena kunci enkripsi dapat disebarkan. Orang-orang dapat menggunakan kunci publik ini, tapi hanya orang yang mempunyai kunci privat sajalah yang bisa mendekripsi data tersebut.

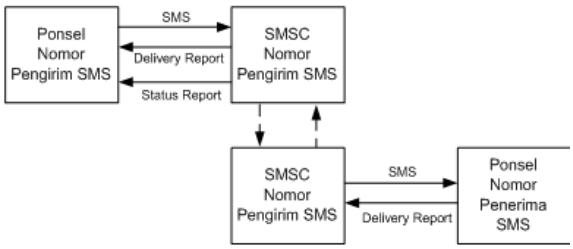
## 2. Landasan Teori

### 2.1 Short Message Service (SMS)

Short Message Service (SMS) adalah kemampuan untuk mengirim dan menerima pesan dalam bentuk teks dari dan kepada ponsel. Teks tersebut bisa terdiri dari kata-kata atau nomor atau kombinasi alphanumeric. SMS diciptakan sebagai standar pesan (message) oleh ETSI (Europesan Telecommunication Standards Institute), yang juga membuat standar GSM yang diimplementasikan oleh semua operator GSM (saat ini standar SMS menjadi tanggung jawab 3GPP - Third Generation Partnership Project). Pada sebuah paket pesan SMS terdiri dari header dan body. Header pesan terdiri dari instruksi-instruksi kepada komponen-komponen yang bekerja dalam jaringan SMS. Pada instruksi-instruksi tersebut, terdapat informasi yang diperlukan selama pengiriman pesan seperti informasi validitas pesan, dan informasi-informasi lainnya. Pada bagian message body, terdapat isi dari pengirim pesan yang akan dikirimkan.



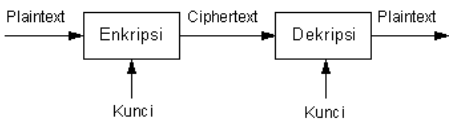

Gambar 2.1 Mekanisme pengiriman SMS dalam satu operator




Gambar 2.2 Mekanisme pengiriman SMS beda operator

### 2.2 Kriptografi

Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula.




Gambar 2.1 Skema Enkripsi dan Dekripsi

### 2.3 RSA

Algoritma RSA, ditemukan oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan enkripsi dan dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Sebuah operasi RSA, baik enkripsi, dekripsi, penandaan, atau verifikasi intinya adalah sebuah eksponensial terhadap modul. Saat ini kriptosistem RSA menggunakan digit minimum sebesar 154 digit (512 bit), hal ini dilakukan untuk menjaga data agar lebih terjaga keamanannya. (Triorizka, 2010)

Secara garis besar, proses kriptografi pada algoritma RSA terdiri dari 3 tahapan yaitu:

1. Pembangkitan Kunci
   - Pilih bilangan prima sembarang *p* dan *q*.
   - Hitung $n = p.q$,
   - Kemudian dicari nilai $\varphi$ yang digunakan untuk mencari kunci publik dan privat menggunakan rumus:
     $\varphi = (p-1)(q-1)$
   - Selanjutnya dicari nilai *e* yang mana diperoleh dari relatif prima antara $\varphi$ dan bilangan yang dicari(*e*) dirutkan menggunakan perulangan yang dimulai dari 2 hingga menemukan relatif prima. Dengan kata lain *e* dan *m* tidak mempunyai faktor prima bersama.
   - Setelah itu dilakukan perhitungan untuk memperoleh nilai *d* untuk dekripsi dengan cara dilakukan perulangan sebanyak 1000 kali untuk mencoba nilai *d* agar memenuhi syarat : e*d mod $\varphi$ hasilnya harus 1.
   - Maka akan didapatkan kunci publik adalah (*n, e*) dan kunci private (*n, d*).
2. Proses Enkripsi
   - Ambil kunci *public* (*n,e*)
   - Ambil plaintext
   - Kemudian tiap karakter tersebut dirubah kedalam format ASCII.
   - Setelah terbentuk dengan format kode ASCII maka dihitung tiap bagian tersebut dengan rumus:
     $ci = mi^e \bmod n$
   - Setelah tiap bagian tersebut terhitung, maka dilakukan penggabungan setiap bagian (*ci*) sehingga memperoleh kesatuan ciphertext c
3. Proses Dekripsi
   - Ambil kunci *privat* (*n,d*)
   - Ambil ciphertext
   - Kemudian dilakukan perhitungan untuk dekripsi dengan rumus:
     $mi = ci^d \bmod n$
   - Pada tahap ini *mi* dikembalikan dari kode ASCII menjadi karakter biasa.
   - Setelah tiap bagian tersebut terhitung, maka dilakukan penggabungan setiap bagian (*mi*) sehingga memperoleh kesatuan plaintext m.

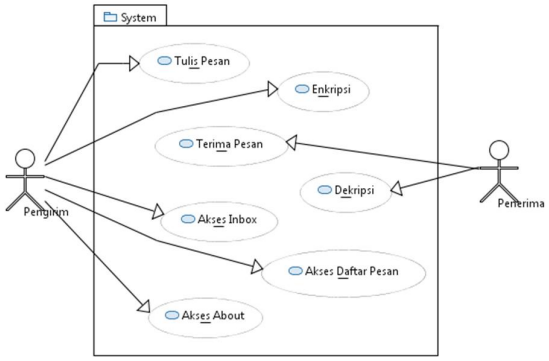
## 3. Perancangan Aplikasi

### 3.1 Gambaran Umum Aplikasi

Aplikasi Enkripsi SMS adalah aplikasi yang dibangun untuk meningkatkan keamanan pertukaran informasi melalui SMS. Sistem ini berguna menjadi alternatif pilihan untuk bertukar pesan secara lebih aman melalui SMS. Angkasa Pura I dalam pencatatan data-data

### 3.2 Use Case Diagram

Use case diagram merupakan pemodelan untuk kelakuan (*behavior*) sistem yang akan dibuat (Rosa A.S., 2013).



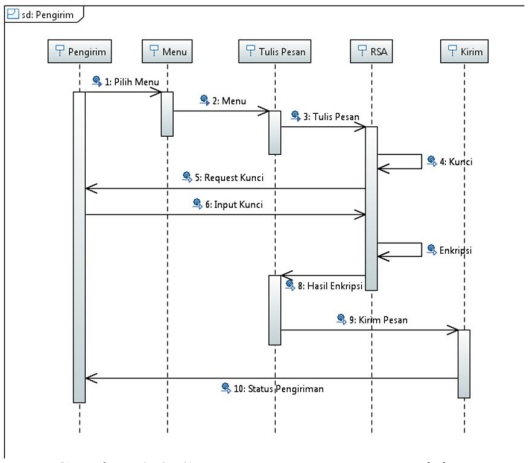

Gambar 3.1 *Use Case* Aplikasi Enkripsi SMS

Pada gambar di atas terdapat 2 aktor yang terdiri dari Pengirim dan Penerima pesan.

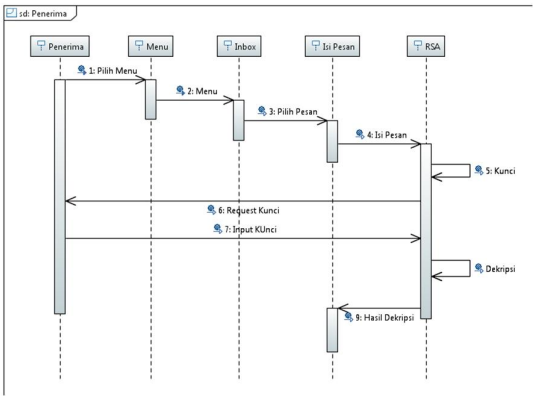
Serta terdapat 7 kelakuan/aktivitas *use case* yang dapat dilakukan oleh aktor yang ada seperti pada gambar 3.3.

### 3.3 Sequence Diagram

Secara umum aplikasi ini terdiri dari dua bagian yang penting yaitu tulis pesan dan baca pesan. Berikut rancangan Sequence Diagram ditunjukkan pada Gambar 3.1 dan Gambar 3.2 :



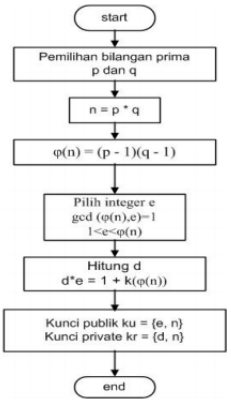

Gambar 3.2 *Sequence Diagram* Pengirim



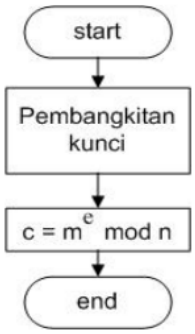

Gambar 3.3 *Sequence Diagram* Penerima

### 3.4 Penerapan RSA

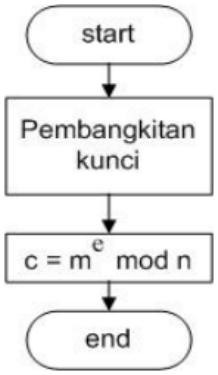
Pada bagian ini akan membahas perancangan untuk pengimplementasian metode ini ke dalam aplikasi sebagai berikut:




Gambar 3.4 Tahapan Pembangkitan Kunci RSA




Gambar 3.5 Tahapan Enkripsi SMS



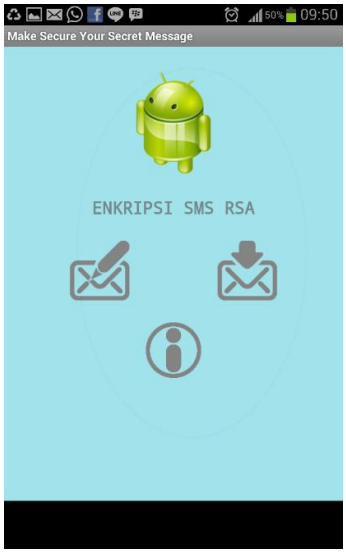
Gambar 3.6 Tahapan Dekripsi SMS

## 4. Implementasi

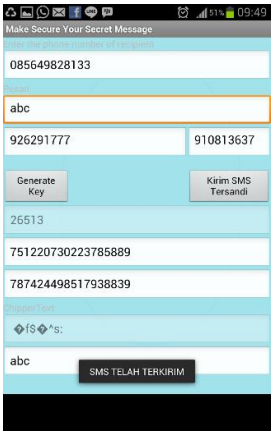
### 4.1 Implementasi Program

Implementasi program yaitu tampilan hasil dari penerapan program yang telah dibuat, sesuai dengan perancangan yang telah dilakukan dengan hasil berupa tampilan aplikasi sebagi berikut:

Implementasi ini Aplikasi Enkripsi SMS dilakukan dengan bahasa pemrograman Java dan berbasis Android.



Gambar 4.1 Halaman Depan



Gambar 4.2 Halaman Tulis Pesan

Gambar 4.3 Halaman Baca Pesan

Gambar 4.1 adalah halaman tampilan awal Alikasi Enkripsi SMS. Terdapat 2 pilihan yaitu Tulis Pesan atau Baca Pesan.

## 5. Pengujian dan Pembahasan

Pengujian pada sistem ini meliputi beberapa jenis pengujian, yaitu pengujian fungsional, pengujian metode den pengujian teknis

### 5.1 Pengujian Fungsional

Untuk menguji kinerja aplikasi dibutuhkan suatu pengujian sistem, yaitu pengujian fungsionalitas aplikasi. Pengujian ini dilakukan dengan cara menjalankan setiap fitur dalam aplikasi dan melihat apakah hasilnya sudah sesuai dengan yang seharusnya. Menurut pengujian sistem yang telah dilakukan, fungsi-fungsi dalam sistem ini telah berjalan sesuai perencanaan

### 5.2 Pengujian Metode

Pada pengujian ini dilakukan dengan cara melakukan percobaan enkripsi dan dekripsi yang dilakukan secara manual dan juga di sistem. Dari hasil pngujian didapati bahwa hasil enkripsi dan dekripsi baik secara manual ataupun di aplikasi sesuai atau sama. Kemudian dilakukan pengujian lebih

lanjut untuk mengetahui tingkat kesuksesan penerapan metode dengan mengambil dari 5 sampel inputan, sehingga menghasilkan grafik sebagai berikut :


Gambar 4.1 Grafik Perbandingan Tiap Nilai

Penjelasan dari gambar diatas yaitu "*Nilai Seharusnya*" yang isinya adalah jumlah karakter awal atau karakter yang akan dilakukan proses enkripsi. Juga terdapat "*Nilai Terukur*" yang isinya adalah jumlah karakter yang sukses setelah karakter awal melalui proses enkripsi dan juga dekripsi oleh sistem. Dalam artian jumlah karakter kembalian setelah melalui enkripsi dan juga dekripsi sesuai dengan karakter awal. Adapula "*Jumlah Karakter Terenkripsi*" meupakan jumlah karakter dari hasil enkripsi yang disimpan ke dalam *database*.

Jadi dapat disimpulkan bahwa penerapan metode kriptografi algoritma RSA untuk proses enkripsi dan dekripsi berhasil diimplementasikan pada sistem dengan tingkat keberhasilan enkripsi dan dekripsi 100% akan tetapi dari hasil uji coba dihasilkan jumlah karakter setelah dilakukan enkripsi mengalami peningkatan. Dibuktikan dari rata-rata peningkatan jumlah karakter setelah dilakukan enkripsi yaitu 3,75 kali dari *text* awal

## 6. Kesimpulan dan Saran

### 6.1 Kesimpulan

Berdasarkan pembahasan sebelumnya dapat ditarik beberapa kesimpulan, yaitu:

a) Berdasarkan uji coba fungsional metode RSA dapat di implementasikan secara baik dalam aplikasi enkripsi dan dekripsi SMS ini. Sehingga aplikasi sms ini telah berhasil menerapkan metode kriptografi menggunakan algoritma RSA untuk pengamanan pertukaran informasi melalui SMS.

b) Hasil pengujian menunjukkan bahwa Aplikasi Enkripsi SMS menggunakan Menggunakan RSA mampu mengacak pesan sehingga sulit untuk dibobol namun jumlah pesan pada SMS mengalami peningkatan. Sehingga untuk memperkecil jumlah pesan terenkrip maka pesan dikembalikan dalam bentuk karakter. Dan dengan pembatasan jumlah pesan maksimal 30 karakter diketahui rata-rata pesan terenkrip sebanyak 23 karakter.

c) Jumlah pesan pada Aplikasi ini tidak bisa lebih besar dari n atau hasil dari p*q

### 6.2 Saran

Berdasarkan penelitian ini, ada beberapa hal yang disarankan, yaitu:

a) Dari proses pengujian metode kriptografi algoritma RSA, didapati bahwa pesan yang mampu di inputkan dan panjang kunci dipengaruhi oleh bitlength yang telah ditentukan sebelumnya. Untuk pengembangan sebaiknya dipikirkan bagaimana jumlah pesan dapat ditingkatkan, namun jumlah kunci dapat di perkecil baik dengan mengkonversi pesan maupun dengan metode yang lain.

b) Menemukan cara pendistribusian kunci yang tepat untuk metode ini.

**Daftar Pustaka:**

Anjari, Becik Gati. 2012. Enkripsi SMS (Short Message Service) pada Telepon Selular Berbasis Android. Surabaya : Politeknik Elektronika Surabaya, Institut Teknologi Sepuluh November.

Arifin, Zainal. 2009. Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. Samarinda: Jurnal Informatika Mulawarman.

Lyracc. 2009. Eclipse IDE. Januari, 7, 2012. http://java.lyracc.com/belajar/java-untukpemula/eclipse-ide.

Nazruddin Safaat H. 2011. Pemograman Android Mobile SmartPhone dan Tablet Pc Berbasis Android. Bandung: INFORMATIKA

Rogers, R. et al. 2009. Android Application Development. Sebastopol: O'Reilly Media Inc.

Wicaksono, Prasetyo Andy. 2007. Studi Pemakaian Algoritma RSA dalam Proses Enkripsi dan Aplikasinya. Bandung : Institut Teknologi Bandung