

# Aplikasi Enkripsi Sms Dengan Metode RSA Pada Smartphone Berbasis Android

I Wayan Dharma Satriawan, I Gusti Made Arya Sasmita, I Putu Agung Bayupati

Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana

Bukit Jimbaran, Bali, Indonesia, telp. +62361703315

email: [satriawan.dharma@yahoo.com](mailto:satriawan.dharma@yahoo.com), [aryasasmita@yahoo.com](mailto:aryasasmita@yahoo.com), [bayupati@ee.unud.ac.id](mailto:bayupati@ee.unud.ac.id)

## Abstrak

Pertukaran informasi melalui SMS digunakan oleh banyak orang. Terkadang informasi yang bersifat rahasia juga dipertukarkan melalui layanan SMS. Pengiriman pesan melalui SMS tidak secara langsung sampai ke penerima pesan, namun SMS terlebih dulu melewati *Short Message Service Center (SMSC)*. SMS rahasia yang dikirimkan dapat diketahui oleh orang yang mempunyai hak akses ke SMSC ataupun oleh orang yang melakukan penyadapan, untuk melindungi pertukaran pesan rahasia melalui SMS perlu adanya aplikasi yang mampu melindungi kerahasiaan pesan yang dikirimkan, dalam hal tersebut ilmu kriptografi dapat digunakan untuk menjaga kerahasiaan pesan, dengan menggunakan algoritma RSA maka pesan dapat dienkripsi untuk keamanan pesan. Aplikasi SMS diterapkan pada *platform* android, karena *platform* android paling banyak digunakan oleh berbagai perangkat *mobile*. Aplikasi yang dibuat mampu melakukan enkripsi dan dekripsi terhadap alfabet, angka dan simbol-simbol. Aplikasi juga mampu melindungi pesan rahasia yang dikirimkan saat dilakukan penyadapan terhadap perangkat *mobile* yang digunakan.

**Kata Kunci:** *Android, Dekripsi, Enkripsi, SMS, Algoritma RSA*

## Abstract

*Exchange of information through SMS are used by many people. Sometimes secret information is also exchanged through SMS service. Sending message via SMS not directly deliver to the receiver of the message, but first SMS pass Short Message Service Center (SMSC). Secret SMS can be known by those who have access to SMSC or by the person doing tapping, to protect the exchange of secret messages via SMS need an application can protect the secret SMS, in this case the science of cryptography can be used to maintain the confidentiality of the message, by using RSA algorithm, then message can be encrypted for security of the message. Application SMS service applied on the Android platform, because android platform most used by mobile device. Applications can doing encryption and decryption of the alphabet, numbers and symbols. Applications are also able to protect secret messages while the mobile device si being tapping.*

**Keywords:** *Android, Encryption, Decryption, SMS, Algoritma RSA.*

## 1. Pendahuluan

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh setiap orang, dan bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi, selain itu pengiriman SMS yang dilakukan tidak sampai ke penerima langsung, akan tetapi pengiriman SMS harus melewati *Short Message Service Center (SMSC)* yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Tersimpannya SMS pada SMSC, maka operator dapat memperoleh informasi atau membaca SMS di dalam SMSC tersebut, hal tersebut dapat dibuktikan dari beberapa kasus yang ditangani pihak kepolisian, kejaksaan dan KPK, dimana pihak-pihak tersebut meminta transkrip SMS ke *operator GSM* untuk dijadikan bahan penyelidikan di persidangan.

Demikian dibutuhkan suatu metode dan aplikasi yang dapat mempertimbangkan solusi encrypted *end to end* dengan melakukan enkripsi terhadap pesan SMS. Enkripsi adalah proses

mengubah suatu pesan asli yang disebut plaintext menjadi sebuah sandi atau kode yang tidak terbaca yang disebut ciphertext dan tidak dapat dimengerti, untuk mengembalikan pesan ke bentuk asli seperti semula diperlukan suatu proses yang disebut dekripsi. Enkripsi dimaksudkan untuk melindungi dan menyamarkan informasi agar tidak terlihat oleh pihak atau orang yang bukan seharusnya.

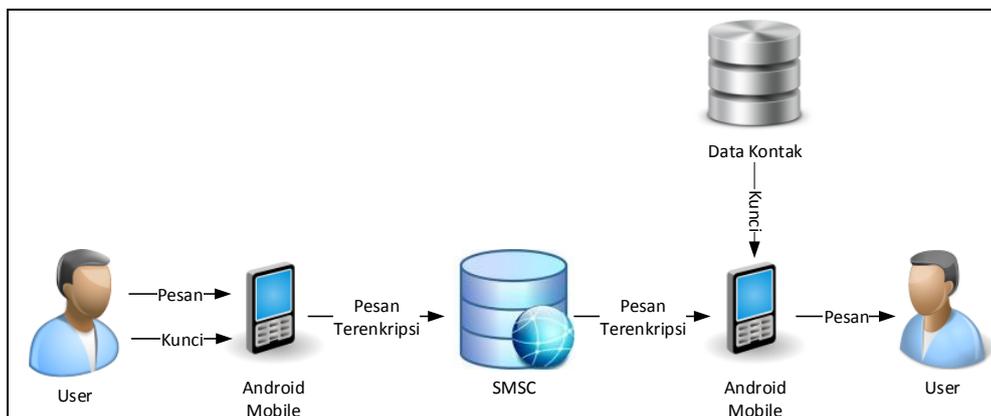
Salah satu metode enkripsi yang umum digunakan yaitu menggunakan algoritma enkripsi dan kunci yang bersifat rahasia. Teknik tersebut disebut sebagai algoritma kunci asimetris yaitu suatu enkripsi dengan menggunakan kunci yang berbeda untuk melakukan proses enkripsi dan dekripsi.

## 2. Metode Penelitian

Metode penelitian yang digunakan untuk memperoleh hasil yang diharapkan dari aplikasi enkripsi SMS adalah mengumpulkan data dan informasi dari sumber-sumber seperti buku, karya tulis, buku digital, internet, dan sumber lain yang berhubungan dengan objek penelitian tentu sangat penting, sehingga studi literatur sangat perlu untuk dilakukan sebagai referensi yang relevan dengan perumusan masalah. Tahap desain terdiri dari beberapa tahapan, yaitu pertama perancangan sistem dan gambaran umum sistem.

### 2.1 Gambaran Umum Sistem

Gambaran umum dari aplikasi enkripsi SMS pada smartphone berbasis android dapat dilihat pada Gambar 1.

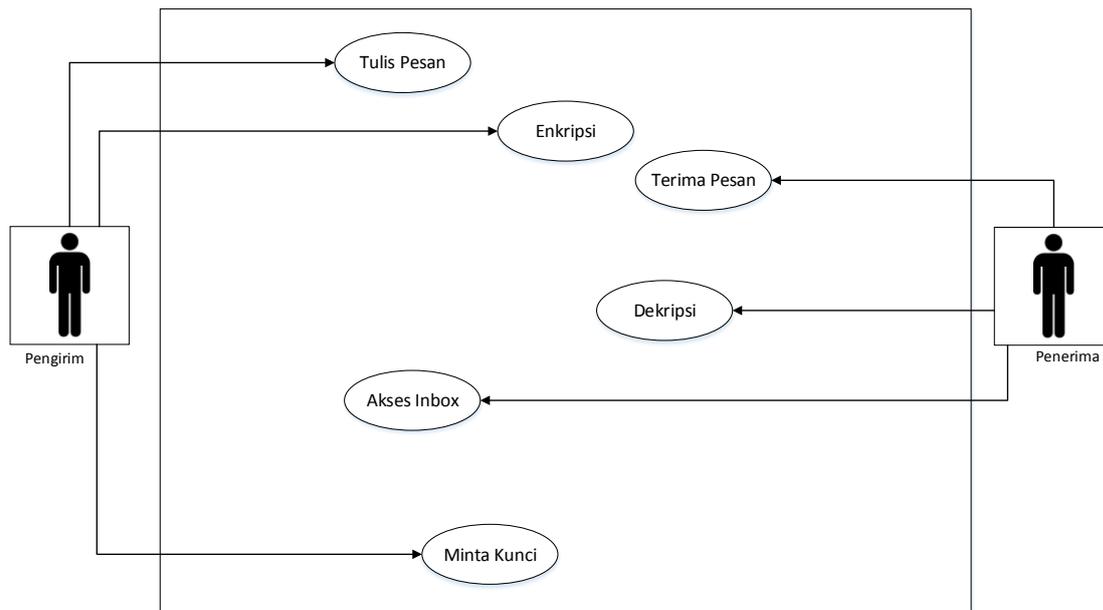


Gambar 1. Gambaran umum aplikasi enkripsi SMS pada smartphone berbasis android

Perangkat lunak yang akan dibangun merupakan perangkat lunak yang diterapkan pada telepon seluler yang bersistem operasi Android dan memiliki fungsi untuk melakukan enkripsi dan dekripsi. Perangkat lunak dapat melakukan pengiriman dan menerima pesan. Pengguna akan berinteraksi dengan perangkat lunak melalui *user interface* yang disediakan oleh perangkat lunak, pengguna memasukkan data dengan menggunakan *keypad* yang dimiliki oleh telepon seluler. Pesan dan kunci untuk enkripsi inputkan oleh user lalu diproses di android mobile milik user pengirim kemudian hasil pesan terenkripsi dikirim melalui jaringan SMS dan pesan diterima di android mobile milik penerima pesan, kemudian sistem mengambil data kunci milik dari user pengirim di data kontak lalu pesan didekripsi kemudian pesan dapat dibaca oleh user penerima.

### 2.2 Use Case Diagram

*Use case diagram* menjelaskan mengenai apa saja yang akan dilakukan oleh aplikasi yang dibuat dan siapa saja yang terlibat dalam interaksi tersebut. *Use case diagram* dari aplikasi enkripsi SMS dapat dilihat pada Gambar 2.



Gambar 2. Use Case diagram

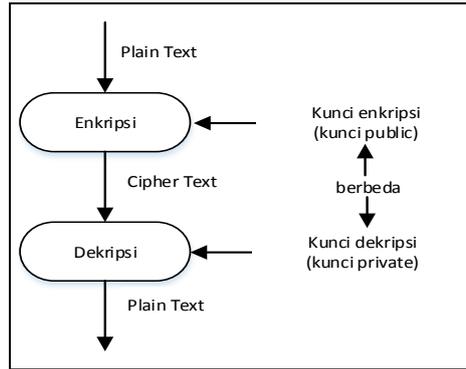
### 3. Kajian Pustaka

#### 3.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti rahasia dan *graphia* berarti tulisan. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Algoritma kriptografi terdiri dari tiga fungsi dasar yaitu enkripsi, dekripsi dan kunci. Keamanan dari kriptografi modern didapat dengan merahasiakan kunci yang dimiliki dari orang lain. tanpa harus merahasiakan algoritma itu sendiri. Kunci memiliki fungsi yang sama dengan password. Jika keseluruhan dari keamanan algoritma tergantung pada kunci yang dipakai maka algoritma tersebut bisa dipublikasikan dan dianalisis oleh orang lain. Jika algoritma yang telah dipublikasikan bisa dipecahkan dalam waktu singkat oleh orang lain maka berarti algoritma tersebut tidaklah aman untuk digunakan [1].

#### 3.2 Algoritma RSA

Algoritma RSA mengambil nama dari Ron Rivest, Adi Shamir dan Len Adleman yang menciptakan metode tersebut pada tahun 1977. Teknik dasarnya ditemukan pertama kali pada tahun 1973 oleh Clifford Cock dari CESG (bagian dari British GCHQ) tetapi dirahasiakan sampai tahun 1977. Paten dimiliki oleh RSA Labs dan telah *expired* [2]. Algoritma RSA adalah enkripsi yang paling umum digunakan dan algoritma otentikasi. Algoritma RSA melibatkan mengalikan dua bilangan prima besar, setelah kunci telah dibuat, bilangan prima asli tidak lagi penting dan dapat dibuang. Baik kunci publik dan kunci privat dibutuhkan untuk enkripsi/dekripsi. Pada algoritma RSA, kunci privat tidak pernah perlu dikirim. Kunci privat digunakan untuk mendekripsi teks yang telah dienkripsi dengan kunci publik [3]. Algoritma kriptografi RSA merupakan algoritma yang termasuk dalam kategori algoritma asimetri bisa disebut juga algoritma kunci publik, disebut algoritma asimetri karena algoritma yang digunakan pada proses enkripsi dan proses dekripsi berbeda dan disebut algoritma kunci publik karena kunci yang digunakan untuk proses enkripsi bisa dipublikasikan dan diketahui oleh banyak orang. Secara umum proses algoritma RSA dapat dilihat pada Gambar 3.



Gambar 3. Proses algoritma RSA

**3.3 SMS(Short Messages Services)**

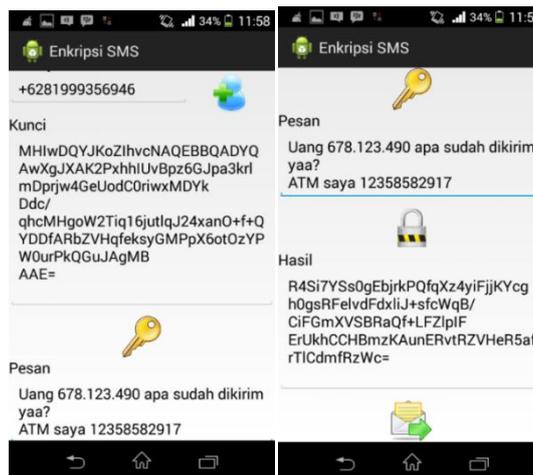
SMS adalah sebuah teknologi yang menyediakan layanan penerimaan dan pengiriman pesan singkat antara perangkat *mobile*. SMS pertama kali dikenalkan di Eropa sekitar tahun 1992, yang pertama kali terintegrasi dalam GSM (*Global System for Mobile, Communications*) yang kemudian berkembang dalam CDMA dan TDMA [4]. Sebuah SMS memiliki batasan karakter yang dapat dikirimkan, 160 karakter jika pengkodean karakter 7-bit yang digunakan dan 70 karakter jika 16-bit Unicode UCS2 (2-byte Universal Character Set) pengkodean karakter yang digunakan [5]. SMS dapat dikirimkan ke perangkat stasiun seluler *digital* lainnya hanya dalam beberapa detik selama berada pada jangkauan pelayanan GSM. SMS dapat memberikan pelayanan apabila pesan yang dikirim tidak sampai ke penerima karena perangkat penerima tidak aktif maupun perangkat penerima diluar jangkauan layanan GSM [6].

Sistem Operasi Mobile Android adalah sistem operasi untuk telepon seluler yang berbasis Linux yang mencakup sistem operasi, middleware, dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi sendiri untuk digunakan oleh bermacam peranti *mobile* [7].

**4. Hasil dan Pembahasan**

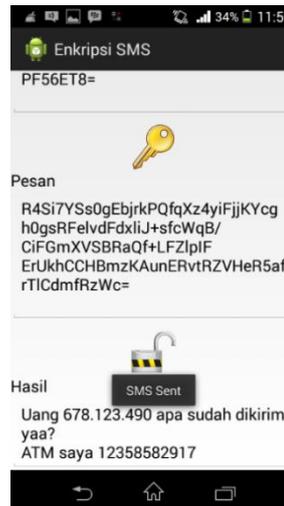
Aplikasi enkripsi SMS tentu harus diuji untuk dapat mengetahui hasil yang didapatkan setelah sistem dijalankan, fungsi utama aplikasi adalah melakukan enkripsi dan deskripsi pesan, sehingga dapat menjaga kerahasiaan satu pesan SMS.

Pengujian dilakukan dengan melakukan enkripsi pesan kemudian pesan akan didekripsi pada sisi penerima pesan. Proses enkripsi pesan dapat dilihat pada Gambar 4 berikut.



Gambar 4. Proses enkripsi pesan

Pesan hasil enkripsi kemudian dikirim lalu akan didekripsi oleh peneriman pesan, proses deskripsi pesan dapat dilihat pada Gambar 5.



Gambar 5. Proses deskripsi pesan

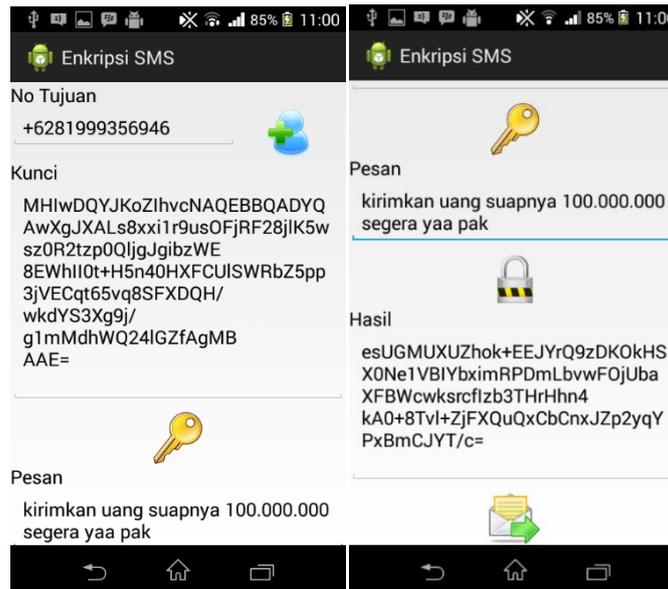
Uji coba enkripsi dan deskripsi pesan dilakukan beberapa kali, hasil dari uji coba dapat dilihat pada tabel 1 berikut.

Tabel 1. Uji coba pesan

No	Pesan	Jumlah Karakter	Hasil Pengujian
1.	Uji coba	8	Berhasil
2.	Tes pesan	9	Berhasil
3.	Aplikasi Android	16	Berhasil
4.	Ibu pergi ke pasar	18	Berhasil
5.	Harga barang itu naik	21	Berhasil
6.	Ani & Budi membeli pakaian	26	Berhasil
7.	Biaya Rp.760.500 harap dibayar	30	Berhasil
8.	ATM saya dibobol, uang saya habis	33	Berhasil
9.	Laporan keuangan ini akan dikumpul	34	Berhasil
10.	Pembayaran Rp.130.985.500 sudah sampai	38	Berhasil
11.	Handphone itu bagus, aku mau beli nanti	39	Berhasil
12.	aku lupa bawa ATM, nanti aku transfer yaa	41	Berhasil
13.	I Wayan Dharma Satriawan, NIM. 10040505038	42	Berhasil
14.	Apakah sudah diterima uang Rp.100.000 nya?	42	Berhasil
15.	Pengiriman paket akan dilakukan pukul 10.00	43	Berhasil
16.	Pembayaran bisa dilakukan jam 09.00 & 14.00	43	Berhasil
17.	2.456 (Dua ribu empat ratus lima puluh enam)	44	Berhasil
18.	Jam 14.30 akan diadakan rapat, harap segera datang.	51	Berhasil
19.	Uang Rp. 120.976.500 sudah dikirim pada 28 Mei 2014	51	Berhasil
20.	Daftar ulang di Universitas Udayana (UNUD), bukit Jimbaran jam 09.00	68	Berhasil
21.	Besok tanggal 20-Mei-2014 tranfer 100.000 rupiah, kalo tidak barang tidak dikirim	81	Berhasil
22.	Pengumuman kelulusan sudah dikeluarkan, jika lulus silakan mendaftar ulang pada tanggal 14-01-2014	98	Berhasil

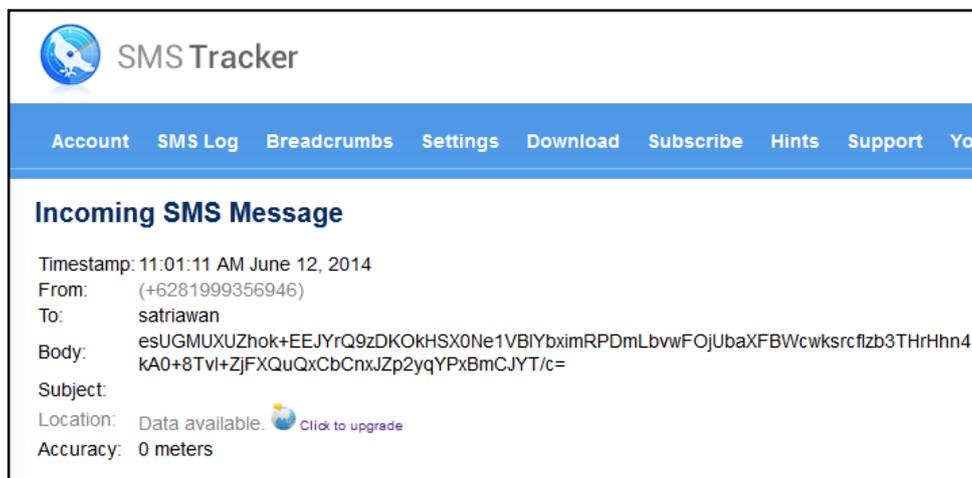
No	Pesan	Jumlah Karakter	Hasil Pengujian
23.	Penggunaan balsem pada keripik pedas sudah banyak ditemui, itu membuat konsumen harus pintar memilih keripik pedas sebelum membeli	130	Berhasil
24.	Piala dunia 2014 diselenggarakan di Brasil, piala dunia akan diselenggarakan selama 1 bulan dan juara bertahan sebelumnya adalah Spanyol	136	Berhasil
25.	Sony merilis ponsel pintar high end miliknya Xperia Z2 beberapa bulan lalu. Terkini, kabarnya Sony juga tengah mengerjakan tiga perangkat terbarunya.	149	Berhasil
26.	Smartphone anyar Motorola, Moto G dengan model 4G LTE dibanderol dengan harga \$219 atau sekitar Rp.2,6 jutaan. Handset ini bisa dibeli langsung melalui website resmi Motorola.	175	Berhasil
27.	Cile memastikan tempat di 16 besar Piala Dunia Brasil, mengikuti langkah Belanda yang terlebih dahulu menang 3-2 atas Australia. Di pertandingan terakhir, Cile tinggal bermain melawan Belanda untuk menentukan juara grup.	220	Berhasil
28.	Setelah secara mengejutkan menelan kekalahan dari Kosta Rika, peluang Uruguay untuk melaju ke babak selanjutnya di Piala Dunia 2014 semakin berat, apalagi sang kapten, Lugano dinyatakan tidak dapat bermain melawan Inggris. Bek West Bromwich Albion itu mengalami cedera lutut.	275	Berhasil
29.	Handset yang memiliki bentang layar 6 inci ini juga diperkuat dengan GPU Adreno 330, sehingga mampu melahap berbagai macam game Android 'berat', termasuk Asphalt 8 dengan pengaturan grafis 'high'. Tidak ada lag atau patah-patah saat modus grafis diposisikan pada tingkat paling maksimal ini dan permainan terasa mulus.	318	Berhasil
30.	Terakhir adalah Pegasus, belum banyak informasi yang menjelaskan rincian mengenai gadget ini. Untuk diketahui, Sony Experia Z3 kabarnya akan diliris pada September di ajang IFA 2014 mendatang. Jadi, untuk Anda para penggemar handset besutan perusahaan yang didirikan oleh Akio Morita ini, masih harus bersabar hingga beberapa bulan ke depan.	341	Berhasil

Pengujian juga dilakukan dengan sebuah aplikasi penyadapan, sebuah pesan dienkripsi kemudian dikirimkan ke penerima, SMS yang dikirimkan dapat dilihat pada Gambar 6.



Gambar 6. Pembuatan pesan penyadapan

Pesan yang dikirimkan akan dilihat pada aplikasi penyadapan yaitu *SMS Tracker*, hasil yang dapat dilihat pada *SMS Tracker* dapat dilihat pada Gambar 7.



Gambar 7. Tampilan pesan di *SMS Tracker*

Hasil yang ditampilkan pada Gambar 7, didapat bahwa *body* atau pesan yang dikirimkan terenkripsi, itu menunjukkan ketika pesan disadap aplikasi dapat menjaga kerahasiaan pesan.

Pengujian juga dilakukan untuk dapat mengetahui karakter apa saja yang dapat dienkripsi oleh aplikasi. Hasil dari uji coba karakter dapat dilihat pada Tabel 2.

Tabel 2. Data uji coba karakter

No	Data Uji Coba	Jumlah Karakter	Hasil Pengujian
1	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLM NOPQRSTUVWXYZ	52	Berhasil
2	1234567890	10	Berhasil
3.	@;_#(\./?!'"=+%*[]{}<> ~^&	30	Berhasil
4.	Uang 678.123.490 apa sudah dikirim yaa? ATM saya 1235852917	59	Berhasil

## 5. Kesimpulan

Percobaan telah yang dilakukan terhadap aplikasi enkripsi SMS, kemudian dapat diambil kesimpulan bahwa aplikasi SMS dapat memberikan keamanan dalam bertukar informasi melalui SMS sehingga tidak dapat dibaca oleh pihak yang tidak berhak, aplikasi juga dapat melakukan enkripsi dan dekripsi pada karakter alfabet, angka dan simbol dan aplikasi juga dapat melakukan enkripsi pesan SMS yang berukuran panjang.

## Daftar Pustaka

- [1] Ariyus,Dony. Pengantar Ilmu Kriptografi.Andi Offset.Yogyakarta. 2008.
- [2] Hendra dan Sukiman. Aplikasi Pengaman Pertukaran SMS pada Perangkat Android dengan Metode RSA. SNASTIKOM. 2012.
- [3] Singh,Sukhjinder dan Majithia,Mr.Sachin. Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA. IJARCSSE.Volume 3. 2013.
- [4] Sunardi.dkk. Aplikasi SMS *Gateway*. Jurnal Teknologi Informasi DINAMIK. Volume XIV, No.1. 2009.
- [5] Saxena,Neetesh dan Payal,Ashish. Enhancing Security System of Short Message Service for M-Commerce in GSM.IJCSET.Volume 2. 2010.
- [6] Wiharto,Yudi. Sistem Informasi Akademik Berbasis Sms *Gateway*. TEKNOMATIKA.Volume I, No. 1. 2011.
- [7] Safaat H, Nazruddin. Android : Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android, Bandung : Informatika. 2012.