PERANCANGAN APLIKASI SMS DENGAN MENGGUNAKAN METODE RSA DAN CAESAR CIPHER BERBASIS ANDROID

SMS Application Design Using RSA and Caesar Method Based On Android

M. Hagi Sandria, Edy Victor Haryanto, Adil Setiawan
[1]Jurusan Sistem Informasi Universitas Potensi Utama
[2,3]Dosen Jurusan Sistem Informasi Universitas Potensi Utama
[1,2,3]Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia - Medan
Email : HagiSandria@gmail.com[1]

ABSTRAK

SMS memiliki banyak celah yang memungkinkan para pencuri untuk mengambilnya. Kelebihan dari SMS ini adalah ketika tujuan sedang sibuk, pesan tetap dapat dikirimkan dengan menyimpan pesan tersebut pada SMSC (Short Message Service Center) dan akan mengirimkan ketika tujuan sudah tidak sibuk. Namun kelebihan ini juga yang menjadikannya kelemahan, dengan tersimpannya pesan pada SMSC, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC tersebut. Untuk itu diperlukan adanya sebuah sistem yang dapat mengamankan isi SMS agar kecurian pesan dapat diatasi. Yaitu dengan menerapkan suatu metode kriptografi pada isi sms. Dengan tersandikannya isi sms, maka seseorang yang berhasil mencuri informasi SMS akan kesulitan untuk mengetahui isi dari SMS tersebut. Untuk itu penulis merekomendasikan metode RSA dan Caesar Cipher sebagai algoritma penyandian isi SMS.

Kata kunci: *RSA, Caesar Cipher, Keamanan, Short Message Service* (*SMS*), *Android, Java, Netbeans*.

ABSTRACT

SMS has many loopholes that allow thieves to take it. The advantage of this SMS is that when the destination is busy, the message can still be sent by saving the message on the SMSC (Short Message Service Center) and will send when the destination is not busy. But this advantage is also the weakness, with the message stored on the SMSC, then the attacker can get a message by infiltration on the SMSC. For that we need a system that can secure the contents of SMS for theft of messages can be overcome. That is by applying a cryptographic method to the content of sms. With tersandikannya content sms, then someone who managed to steal SMS information will be difficult to know the contents of the SMS. For that the authors recommend the RSA and Caesar Cipher method as an SMS content encryption algorithm.

Keyword: *RSA, Caesar Cipher, Keamanan, Short Message Service* (*SMS*), *Android, Java, Netbeans*.

1. PENDAHULUAN

SMS memungkinkan pengguna *handphone* untuk mengirim pesan singkat kepada pengguna *handphone* yang lain dengan cepat dan hanya menggunakan biaya yang sedikit. SMS memiliki banyak celah yang memungkinkan para pencuri untuk mengambilnya. Kelebihan dari SMS ini adalah ketika tujuan sedang sibuk, pesan tetap dapat dikirimkan dengan menyimpan pesan tersebut pada SMSC (*Short Message Service Center*) dan akan mengirimkan ketika tujuan sudah tidak sibuk. Namun kelebihan ini

juga yang menjadikannya kelemahan, dengan tersimpannya pesan pada SMSC, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC tersebut.

Untuk itu diperlukan adanya sebuah sistem yang dapat mengamankan isi SMS agar kecurian pesan dapat diatasi. Yaitu dengan menerapkan suatu metode kriptografi pada isi *sms*. Dengan tersandikannya isi *sms*, maka seseorang yang berhasil mencuri informasi SMS akan kesulitan untuk mengetahui isi dari SMS tersebut. Untuk itu penulis merekomendasikan metode RSA dan *Caesar Cipher* sebagai algoritma penyandian isi *sms*. 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. 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. Dalam kriptografi, Sandi *Caesar*, atau Sandi Geser, Kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Pada *Caesar Cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). Akan tetapi kriptografi tersebut tidak akan berjalan tanpa adanya aplikasi tambahan pada telepon genggam yang digunakan. Untuk itu, digunakan bahasa pemrograman *Java Android* dan menggunakan *Netbeans* sebagai IDE (*Integrated Environtment Development*) dan juga *emulator* sebagai tampilan hasil eksekusinya.

2. METODOLOGI PENELITIAN

Adapun metodologi penelitian yang digunakan penulis pada penelitian ini adalah :

1. Metode Penelitian Lapangan *(Field Research)*

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

1.1. Pengumpulan Data

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

a. Pengamatan Langsung (Observation)

Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian-bagian terpenting dalam pengambilan data yang diperlukan berkaitan tentang kriptografi dan SMS.

b. Wawancara (Interview)

Teknik ini secara langsung bertatap muka dengan ahli kriptografi untuk mendapatkan penjelasan dari masalah-masalah yang sebelumnya kurang jelas yaitu kriptografi dan juga untuk meyakinkan bahwa data yang diperoleh dikumpulkan benar-benar akurat.

c. Sampling

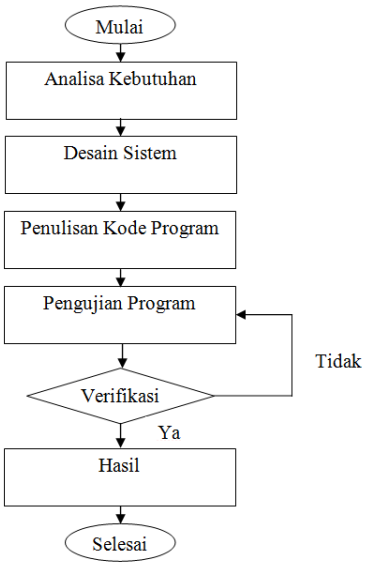
Meneliti dan memilih data-data yang tersedia dan sesuai dengan bidang yang dipilih sebagai berkas lampiran.

2. Penelitian perpustakaan (Library Research)

Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori.

3. Flowchart Metode Penelitian

Berikut adalah flowchart metode penelitian yang digunakan dalam penelitian ini.



Gambar 1. Flowchart Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data tentang kriptografi dan SMS.

Pada tahapan ini juga ditentukan software dan hardware yang akan digunakan untuk mengimplementasikan dan menguji hasil penelitian. Berdasarkan data-data yang ada ini kemudian dilakukan tahap selanjutnya, yaitu desain sistem.

Berikut adalah software yang digunakan untuk pembuatan sistem :

a. Sistem operasi windows 7
b. Netbeans 8.0
c. Android Emulator

Berikut adalah hardware yang digunakan untuk penerapan sistem :

a. Laptop/ Computer
b. Hardisk
c. USB Cable

2. Desain Sistem

Proses desain akan menerjemahkan syarat kebutuhan sebuah perancangan perangkat lunak yang dapat diperkirakan sebelum dibuat kode program. Proses ini berfokus kepada : struktur data, arsitektur perangkat lunak, representasi interface, dan detail (algoritma) prosedural. Dokumen inilah yang akan digunakan untuk melakukan aktivitas pembuatan sistemnya. Pada tahap ini dilakukan desain perangkat lunak menggunakan pemodelan uml yaitu use case diagram, class diagram, activity diagram dan sequence diagram.

3. Penulisan Kode Program

Kode program merupakan terjemahan design dalam bahasa yang bisa dikenali komputer. Pada tahap ini desain sistem diimplementasikan ke dalam kode program. Pemrograman dimulai dengan bahasa pemrograman java android dan xml.

4. Pengujian Program

Pengujian program merupakan langkah yang dilakukan setelah penulisan kode program. Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahap ini program akan diterapkan untuk mengamankan pesan pendek pada perangkat android. Kemudian program secara otomatis akan menampilkan hasil dari perancangan sistem. Aplikasi ini menampilkan teks SMS yang tersandikan dan yang belum tersandikan.

3. HASIL DAN PEMBAHASAN

3.1. Penerapan Metode

Pada perancangan Aplikasi SMS Dengan Menggunakan Metode RSA Dan *Caesar Cipher* Berbasis *Android* dibutuhkan sebuah perhitungan yang sesuai dengan metode yang digunakan. Adapun rumus dan perhitungan metode yang digunakan adalah sebagai berikut :

3.1.1. Metode RSA

1. Enkrip Metode RSA

   Berikut ini adalah enkrip dari metode RSA, enkrip metode RSA menggunakan fungsi eksponensial dalam modular *n* sebagai berikut :

   $C_i = P_i^e \ mod \ n$

   Keterangan :

   C_i = *Ciphertext* hasil enkrip
   P_i = *Plaintext* yang akan dienkrip
   e = Fungsi eksponensial
   mod = Sisa Bagi/Modulus
   n = Hasil perkalian dua buah bilangan prima

2. Pembentukan Kunci :

a. Menentukan dua buah bilangan prima

Tentukan dua buah bilangan prima besar dengan ketentuan kedua bilangan prima tidak boleh sama.

$P_1 = 31$
$P_2 = 37$

b. Mencari nilai n

Untuk mendapatkan nilai n, maka gunakan rumus berikut :

$n = P_1 \times P_2$
$= 31 \times 37$
$= 1147$

c. Mencari nilai 0n

Untuk mencari nilai 0n gunakan rumus berikut :

- $0n = (P_1 - 1) \times (P_2 - 1)$
- $0n = (31 - 1) \times (37 - 1)$
- $0n = 30 \times 36$
- $0n = 1080$

d. Mencari nilai e

Untuk menentukan nilai e, gunakan algoritma berikut :

e = 2
While 0n mod e ≠ 0
e = e + 1
End While

Artinya :

Sampai 0n mod e ≠ 0, lakukan e = e + 1. Proses berhenti ketika nilai 0n dibagi dengan nilai e memiliki sisa bagi tidak sama dengan nilai 0, maka akan didapat nilai e.

e = 3

Iterasi Pertama :

- 0n mod e = 1080 mod 3
  = 0

e = 3 + 1
e = 4

Iterasi Kedua :

- 0n mod e = 1080 mod 4
  = 0

e = 4 + 1
e = 5

Proses berhenti ketika $V_3 = 0$, maka telah didapat nilai d = 463.
Maka telah diperoleh kunci *private* untuk enkrip sebagai berikut :
e = 7
n = 1147
Dan diperoleh kunci *public* untuk dekrip sebagai berikut :
d = 463
n = 1147
2. Enkrip *Plaintext*
Contoh Proses Enkrip :
Plaintext : POTENSI UTAMA
Enkrip Pertama :
P = 80
$C_i = P_i^e \bmod n$
$= 80^7 \bmod 1147$
$= 20971520000000 \bmod 1147$
$= 660$
Enkrip Kedua :
O = 79
$C_i = P_i^e \bmod n$
$= 79^7 \bmod 1147$
$= 19203908986159 \bmod 1147$
$= 1128$
Enkrip Ketiga :
T = 84
$C_i = P_i^e \bmod n$
$= 84^7 \bmod 1147$
$= 29509034655744 \bmod 1147$
$= 269$
Enkrip Keempat :
E = 69
$C_i = P_i^e \bmod n$
$= 69^7 \bmod 1147$
$= 7446353252589 \bmod 1147$
$= 648$
Enkrip Kelima :
N = 78
$C_i = P_i^e \bmod n$
$= 78^7 \bmod 1147$
$= 17565568854912 \bmod 1147$
$= 659$
Enkrip Keenam :
S = 83
$C_i = P_i^e \bmod n$
$= 83^7 \bmod 1147$
$= 27136050989627 \bmod 1147$
$= 941$
Enkrip Ketujuh :
I = 73
$C_i = P_i^e \bmod n$
$= 73^7 \bmod 1147$
$= 11047398519097 \bmod 1147$
$= 850$
Enkrip Kedelapan :
$= 32$
$C_i = P_i^e \bmod n$

$= 32^7 \bmod 1147$
$= 34359738368 \bmod 1147$
$= 1055$

Enkrip Kesembilan :
U = 85
$C_i = P_i^e \bmod n$
$= 85^7 \bmod 1147$
$= 32057708828125 \bmod 1147$
$= 122$

Enkrip Kesepuluh :
T = 84
$C_i = P_i^e \bmod n$
$= 84^7 \bmod 1147$
$= 29509034655744 \bmod 1147$
$= 269$

Enkrip Kesebelas :
A = 65
$C_i = P_i^e \bmod n$
$= 65^7 \bmod 1147$
$= 4902227890625 \bmod 1147$
$= 761$

Enkrip Kedua belas :
M = 77
$C_i = P_i^e \bmod n$
$= 77^7 \bmod 1147$
$= 16048523266853 \bmod 1147$
$= 1077$

Enkrip Ketiga belas :
A = 65
$C_i = P_i^e \bmod n$
$= 65^7 \bmod 1147$
$= 4902227890625 \bmod 1147$
$= 761$

b. Dekrip Metode *RSA*

Berikut ini adalah dekrip dari metode *RSA*, dekrip metode *RSA* merupakan fungsi eksponensial dalam modular n dengan menggunakan kunci *private* sebagai berikut :

$$P_i = C_i^d \bmod n$$

Keterangan :
P_i = *Plaintext* hasil dekrip
C_i = *Ciphertext* yang akan didekrip
d = Fungsi eksponensial kunci *public*
mod = Sisa Bagi/Modulus
n = Fungsi perkalian dua bilangan prima

1. Terima kunci
d = 463
n = 1147

2. Dekrip *Ciphertext*

Contoh Proses Dekrip :
Dekrip Pertama :
C = 660
$P_i = C_i^d \bmod n$
$= 660^{463} \bmod 1147$
$= 2{,}810879032129157273168565612080 5e+1305 \bmod 1147$
$= 80 = P$

Dekrip Kedua :

C = 1128
$P_i = C_i^d \bmod n$
$= 1128^{463} \bmod 1147$
= 1,656201359164289833094731671496 3e+1413 mod 1147
= 79 = O
Dekrip Ketiga :
C = 269
$P_i = C_i^d \bmod n$
$= 269^{463} \bmod 1147$
= 9,447255068259840601634893182 32e+1124 mod 1147
= 84 = T
Dekrip Keempat :
C = 648
$P_i = C_i^d \bmod n$
$= 648^{463} \bmod 1147$
= 5,744175735220589484373442905 2717e+1301 mod 1147
= 69 = E
Dekrip Kelima :
C = 659
$P_i = C_i^d \bmod n$
$= 659^{463} \bmod 1147$
= 1,392986658792430704663252958 6711e+1305 mod 1147
= 78 = N
Dekrip Keenam :
C = 941
$P_i = C_i^d \bmod n$
$= 941^{463} \bmod 1147$
= 5,915557046472247595367728069 406e+1376 mod 1147
= 83 = S
Dekrip Ketujuh :
C = 850
$P_i = C_i^d \bmod n$
$= 850^{463} \bmod 1147$
= 2,093932153165143283083059356 5398e+1356 mod 1147
= 73 = I
Dekrip Kedelapan :
C = 1055
$P_i = C_i^d \bmod n$
$= 1055^{463} \bmod 1147$
= 5,832957477385789945130796932 8469e+1399 mod 1147
= 32 =
Dekrip Kesembilan :
C = 122
$P_i = C_i^d \bmod n$
$= 122^{463} \bmod 1147$
= 9,651650840205358246697375194 2321e+965 mod 1147
= 85 = U
Dekrip Kesepuluh :
C = 269
$P_i = C_i^d \bmod n$
$= 269^{463} \bmod 1147$
= 9,447255068259840601634893182 32e+1124 mod 1147
= 84 = T
Dekrip Kesebelas :
C = 761

$P_i = C_i^d \bmod n$
$= 648^{463} \bmod 1147$
$= 5{,}744175735220589484373442905271 7e+1301 \bmod 1147$
$= 65 = A$
Dekrip Kedua belas :
C = 1077
$P_i = C_i^d \bmod n$
$= 1077^{463} \bmod 1147$
$= 8{,}238926470782347878069839749415 2e+1403 \bmod 1147$
$= 77 = M$
Dekrip Ketiga belas :
C = 761
$P_i = C_i^d \bmod n$
$= 761^{463} \bmod 1147$
$= 1{,}205302576080124233272239658930 4e+1334 \bmod 1147$
$= 65 = A$
Plaintext : POTENSI UTAMA

2. Metode Caesar Cipher
Algoritma enkripsi *caesar cipher* :
Ci = Pi + 3
Algoritma dekripsi *caesar cipher* :
Pi = Ci - Ki
Contoh Proses Enkripsi :
Plaintext : POTENSI
Solusi :
Ascii Plaintext :
P = 80
O = 79
T = 84
E = 69
N = 78
S = 83
I = 73
C1 = P + 3
= 80 + 3
= 83
= S
C2 = O + 3
= 79 + 3
= 82
= R
C3 = T + 3
= 84 + 3
= 87
= W
C4 = E + 3
= 69 + 3
= 72
= H
C5 = N + 3
= 78 + 3
= 81
= Q
C6 = S + 3

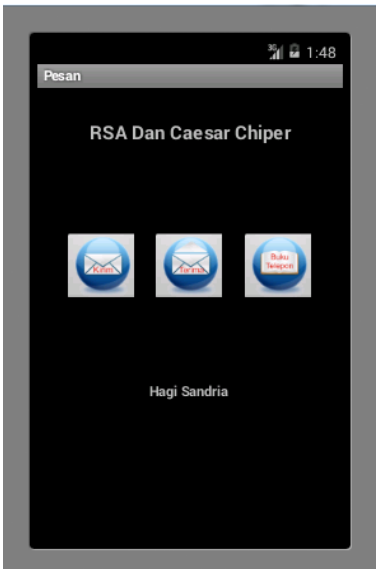
= 83 + 3
= 86
= V
C7 = I + 3
= 73 + 3
= 76
= L
Chipertext : SRWHQVL

Contoh Proses Dekripsi :
P1 = S - 3
= 83 – 3
= 80
= P
P2 = R - 3
= 82 - 3
= 79
= O
P3 = W - 3
= 87 - 3
= 84
= T
P4 = H - 3
= 72 - 3
= 69
= E
P5 = Q - 3
= 81 - 3
= 78
= N
P6 = V - 3
= 86 - 3
= 83
= S
P7 = L - 3
= 76 - 3
= 73
= I
Plaintext : POTENSI

Aplikasi yang dibuat diberi nama perancangan aplikasi sms dengan menggunakan metode rsa dan caesar cipher berbasis android. Aplikasi tersebut merupakan sebuah aplikasi android yang dirancang dengan menggunakan netbeans.

1. *Form* Halaman Utama

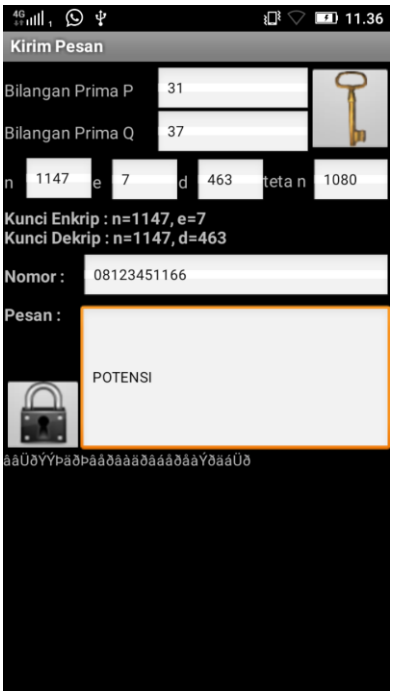
Tampilan berikut adalah interface form halaman utama aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat dilihat pada gambar berikut :



Gambar 2. Halaman Utama

2. *Form* Enkrip/Penyandian Pesan

Tampilan berikut adalah interface form enkrip/penyandian pesan utama aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat dilihat pada gambar berikut :



Gambar 3. Form Enkrip/Penyandian Pesan

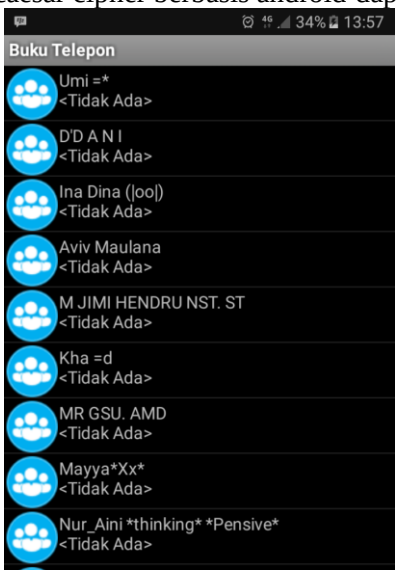
3. *Form* Form Dekrip/Buka Pesan

Tampilan berikut adalah interface form dekrip/buka pesan panduan aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat dilihat pada gambar berikut :

Gambar 4. Form Form Dekrip/Buka Pesan

4. *Form* Kontak/Buku Telepon

Tampilan berikut adalah interface form tampilan kontak/buku telepon aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat dilihat pada gambar berikut :



Gambar 5. Form Kontak/Buku Telepon

Tabel 1. Hasil Enkrip/Kirim Pesan Dengan Metode RSA

No	Pesan Asli	Bilangan prima p	Bilangan prima Q	Hasil Enkripsi
1	POTENSI	31	37	βäðäþåäÞããðããðÝÜßäðäääðÝÝäð

Tabel 2. Hasil Enkrip/Kirim Pesan Dengan Metode Caesar Cipher

No	Pesan Asli	Kunci	Hasil Enkripsi
1	POTENSI	3	SRVHQVL

4. KESIMPULAN

Berdasarkan hasil perancangan aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android yang telah dibuat oleh penulis, maka dapat diambil kesimpulan sebagai berikut :

1. Dengan menggunakan Netbeans 8.0 dengan bahasa pemrograman java dan XML dapat menghasilkan aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android.
2. Metode metode RSA dan caesar cipher dapat merubah pesan SMS asli menjadi pesan SMS sandi dengan perhitungan berdasarkan rumus metode masing-masing.
3. Aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat memiliki keamanan yang baik.

5. SARAN

Berdasarkan hasil kesimpulan diatas, maka penulis membuat beberapa saran, yaitu :

1. Aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat menyandikan teks pesan yang lain pada android, misalnya Line, BBM dan lain sebagainya.
2. Aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat menggunakan metode lain yang penyandiannya lebih kuat.
3. Aplikasi SMS dengan menggunakan metode RSA dan caesar cipher berbasis android dapat diterapkan berbasis online.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Universitas Potensi Utama yang telah banyak membantu penulis dalam menyelesaikan laporan penelitian ini. :

DAFTAR PUSTAKA

[1] Sitohang, dkk, 2013, *Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook Dengan Algoritma Des. STMIK Budi Darma. Medan.*

[2] Azanuddin, dkk, 2013, *Penyandian Short Message Service (SMS) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld*. elita Informatika Budi Darma, ISSN : 2301-9425.

[3] Sholeh, dkk, 2013, *Mengamankan Skrip Pada Bahasa Pemrograman PHP Dengan Menggunakan Kriptografi Base64*. Sekolah Tinggi Teknologi Garut, Garut.

[4] Satriawan, dkk, 2014, *Aplikasi Enkripsi Sms Dengan Metode RSA Pada Smartphone Berbasis Android*, Universitas Udayana, Jurnal Merpati, Vol. 2, No. 2.

[5] Seftyanto, dkk, 2012, *Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi*, Sekolah Tinggi Sandi Negara, Jurnal Prosiding, Vol. 1, No. 1.

[6] Sanjaya, 2014, *Sistem Informasi Geografis Letak Kolam Renang Umum Di Kota Medan Berbasis Android*, STMIK Potensi Utama, Jurnal Seminar Teknik Informatika, Vol. 1, No. 1.