

**APLIKASI *E-VOTING* BUPATI KABUPATEN BANGKA  
MENGUNAKAN ALGORITMA RSA BERBASIS ANDROID**

**SKRIPSI**



Oleh:

AHMAD RAMADHANI

1411500040

**PROGRAM STUDI TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**ATMALUHUR  
PANGKALPINANG**

**2017/2018**

**APLIKASI *E-VOTING* BUPATI KABUPATEN BANGKA  
MENGUNAKAN ALGORITMA RSA BERBASIS ANDROID**

**SKRIPSI**

**Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer**



**PROGRAM STUDI TEKNIK INFORMATIKA  
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN  
KOMPUTER ATMALUHUR  
PANGKALPINANG  
2017/2018**

## LEMBARAN PERYATAAN

Yang bertanda tangan di bawah ini:

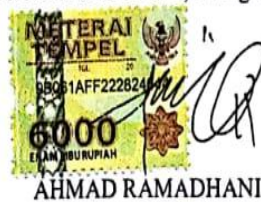
NIM : 1411500040

Nama : AHMAD RAMADHANI

JudulSkripsi : APLIKASI *E-VOTING* MENGGUNAKAN ALGORITMA RSA  
BERBASIS ANDROID

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

PANGKALPINANG, 15 Agustus 2018

  
AHMAD RAMADHANI

**LEMBAR PENGESAHAN SKRIPSI**

**APLIKASI E-VOTING BUPATI KABUPATEN BANGKA  
MENGUNAKAN ALGORITMA RSA BERBASIS ANDROID.**

Yang dipersiapkan dan disusun oleh

**AHMAD RAMADHANI  
1411500040**


Telah dipertahankan di depan Dewan Penguji  
Pada Tanggal 20 Agustus 2018

**Anggota**



**Eza Budi Perkasa, M.Kom  
NIDN. 0201089201**

**Dosen Pembimbing**



**Dwi Yuny Sylfania, M.Kom  
NIDN. 0207069301**

**Kaprodi Teknik Informatika**

  
**R. Burham Isnanto F., S.Si, M.Kom  
NIDN. 0224048003**

**Ketua**



**Yohanes Setiawan, M.Kom  
NIDN. 0219068501**

Skripsi ini telah diterima dan sebagai salah satu persyaratan  
Untuk memperoleh gelar Sarjana Komputer  
Tanggal 24 Agustus 2018

**KETUA SEMK ATMA LUHUR PANGKALPINANG**



**Dr. Husni Teja Sukmana, ST., M.Sc  
NIP. 197710302001121003**

## KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika STMIK Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta yang telah memberi dukungan kepada penulis.
3. Bapak Drs. Djaetun HS yang telah mendirikan STMIK Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, ST., M.Sc, selaku Ketua STMIK Atma Luhur.
5. Bapak R.Burham Isnanto Farid, S.Si., M. Kom, Selaku Kaprodi Teknik Informatika.
6. Ibu Dwi Yuny Sylfania, M.Kom selaku dosen pembimbing penulis.
7. Saudara dan sahabat-sahabatku terutama kawan-kawan angkatan 2014 yang telah memberikan dukungan moral untuk terus menyelesaikan skripsi ini.

Semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Pangkalpinang, 11 Agustus 2018

AHMAD RAMADHANI



## **ABSTRACT**

*Development of technology for several years is very rapidly. Electoral technology such as e-voting is often used in the community. But in terms of the security of the data has not been established although it posted to the database. What's more the election his vote using manual selection, very many will risk where data can be selected in sound manipulation by irresponsible parties at the time of the delivery of data to the Centre and also a lot of cost, because sending data from the election results is done gradually and use transfortasi to deliver the data to the national results Centre. There is therefore the issue then needed an application. By using the Cryptografy algorithm RSA to do the election so that data from voters being safe. This model is one of the key algorithm symmetrically shaped block ciphers that can respond to data security. The method is suitable for maintaining the security of the data. In this paper discussed a number of aspects of Cryptography and the concept of the algorithm RSA. An application designed to be able to implement the RSA algorithm on a smartphone android expected to encrypt data before it is sent to the database. By using the application 's e-voting districts employ algorithms RSA data security of the electorate could be safer and more cost-effective.*

*Keywords: e-voting, cryptography RSA, regional head, android,*



## ABSTRAK

Perkembangan teknologi untuk beberapa tahun ini sangat pesat. Teknologi pemilihan seperti *e-voting* sering digunakan di masyarakat. Tapi dari segi keamanan dari data pemilihan tersebut belum terjamin meskipun dikirim di *database*. Apa lagi pemilihan suaranya menggunakan pemilihan manual, sangat banyak akan resiko yang dimana data suara yang dipilih bisa di manipulasi oleh pihak yang tidak bertanggung jawab pada saat melakukan pengiriman data ke pusat dan juga banyak memakan biaya, karena pengiriman data dari hasil pemilu dilakukan secara bertahap dan menggunakan transportasi untuk mengantar data hasil pemili ke pusat. Oleh karena ada persoalan tersebut maka diperlukan sebuah aplikasi. Dengan menggunakan algoritma kriptografi RSA untuk melakukan pemilihan agar data dari pemilih menjadi aman. Model ini merupakan salah satu algoritma kunci *simetris* yang berbentuk *block chiper* yang dapat menjawab keamanan data. Metode tersebut sangat cocok untuk menjaga keamanan data. Pada tulisan ini dibahas sejumlah aspek dari kriptografi serta konsep dari algoritma RSA. Sebuah aplikasi dirancang untuk dapat mengimplementasikan algoritma RSA pada *smartphone* android diharapkan dapat mengenkripsi data sebelum dikirim ke *database*. Dengan menggunakan aplikasi *e-voting* kepala daerah menggunakan algoritma RSA, keamanan data dari pemilih bisa menjadi lebih aman dan lebih hemat biaya.

Kata kunci : *e-voting*, kriptografi RSA, kepala daerah, android,



## DAFTAR ISI

	Halaman
<b>LEMBAR PERNYATAAN .....</b>	<b>i</b>
<b>LEMBAR PERSETUJUAN .....</b>	<b>ii</b>
<b>KATA PENGANTAR.....</b>	<b>iii</b>
<b>ABSTRACT.....</b>	<b>iv</b>
<b>ABSTRAK .....</b>	<b>v</b>
<b>DAFTAR ISI.....</b>	<b>vi</b>
<b>DAFTAR GAMBAR.....</b>	<b>ix</b>
<b>DAFTAR TABEL.....</b>	<b>xi</b>
<b>DAFTAR SIMBOL .....</b>	<b>xii</b>
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian .....	4
1.5 Sistematika Penulisan.....	4
<b>BAB II LANDASAN TEORI</b>	
2.1 Kriptografi.....	6
2.2 Android.....	7
2.2.1 Sejarah Android.....	8
2.2.2 Versi Android.....	9
2.2.3 Arsitektur Android .....	11
2.2.4 Android SDK ( <i>Software Development Kit</i> ).....	11
2.2.5 Android ADT ( <i>Android Development Tools</i> ).....	12
2.3 <i>Eclipse</i> .....	13
2.4 <i>Java</i> .....	14
2.5 PHP.....	14



2.6	RSA ( <i>Rivert Shamir Adleman</i> ).....	15
2.6.1	Contoh Soal Algoritma RSA.....	16
2.7	<i>E-Voting</i> .....	17
2.7.1	Kelebihan <i>E-Voting</i> .....	18
2.7.2	Kelemahan <i>E-Voting</i> .....	19
2.8	Model Pengembangan Sistem .....	20
2.8.1	Tahap-Tahap Dalam Pemodelan <i>WaterFall</i> .....	20
2.8.2	Keunggulan Model <i>Waterfall</i> .....	22
2.8.3	Kelemahan Model <i>Waterfall</i> .....	22
2.9	Motode Pengembangan Perangkat Lunak.....	22
2.10	Tools Pengembangan Sistem.....	24
2.10.1	<i>Use Case Diagram</i> .....	25
2.10.2	<i>Activity Diagram</i> .....	25
2.10.3	<i>Squence Diagram</i> .....	27
2.10.4	<i>Class Diagram</i> .....	27
2.11	Penelitian Terdahulu .....	28
 <b>BAB III METODOLOGI PENELITIAN</b>		
3.1	Model Pengembangan Sistem.....	33
3.2	Metode Pengembangan Sistem .....	34
3.3	<i>Tools</i> Pengembangan Sistem.....	35
 <b>BAB IV HASIL DAN PEMBAHASAN</b>		
4.1	Analisis Masalah .....	36
4.1.1	Analisis Kebutuhan .....	36
4.1.2	Analisa Proses .....	38
4.1.3	Analisa Sistem Berjalan .....	39
4.1.4	Analisa Sistem Usulan .....	39
4.2	Perancangan Sistem .....	40
4.2.1	Identifikasi Sistem Usulan .....	40
4.2.2	Rancangan Sistem.....	40

4.2.3 Perancang <i>Interface</i> Aplikasi.....	60
4.3 Implementasi.....	66
4.4 Penerapan Algoritma.....	75
4.4.1 Analisa Penerapan Algoritma RSA Pada Aplikasi .....	75
4.5 Pengujian Sistem.....	76
4.5.1 Pengujian Sistem Menggunakan <i>Blackbox</i> .....	76
4.5.2 Hasil Pengujian Sistem Menggunakan <i>Wireshark</i> .....	77

## **BAB V PENUTUP**

5.1 Kesimpulan .....	78
5.2 Saran.....	78

<b>DAFTAR PUSTAKA</b> .....	79
-----------------------------	----

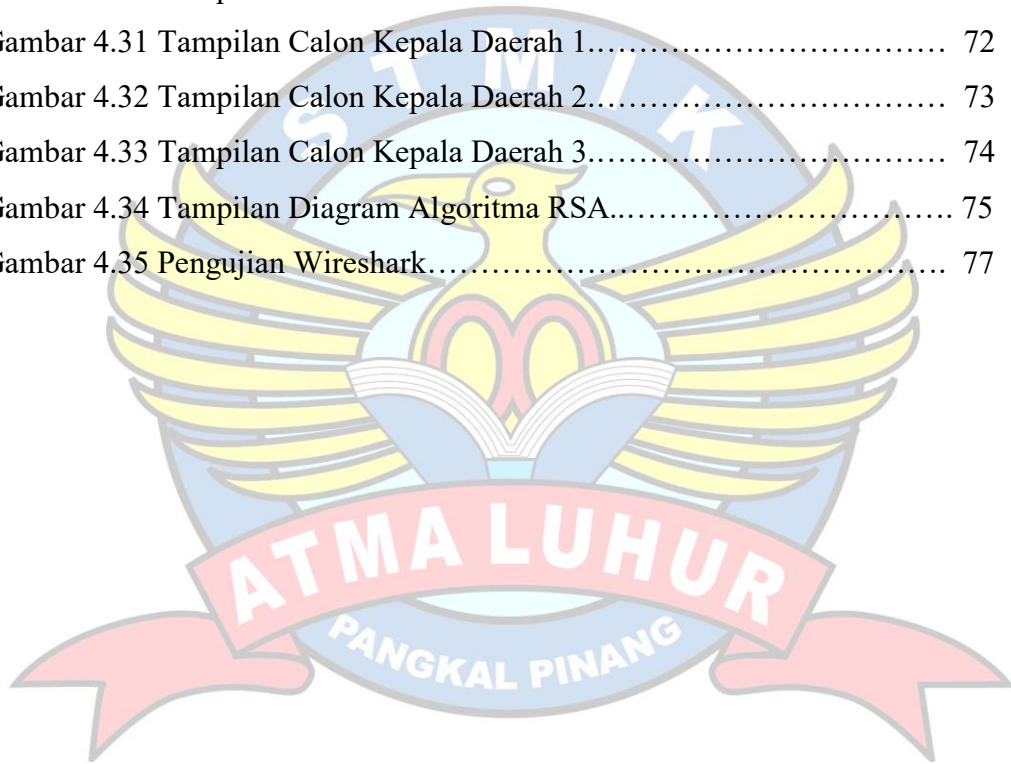
<b>LAMPIRAN</b> .....	
-----------------------	--



## DAFTAR GAMBAR

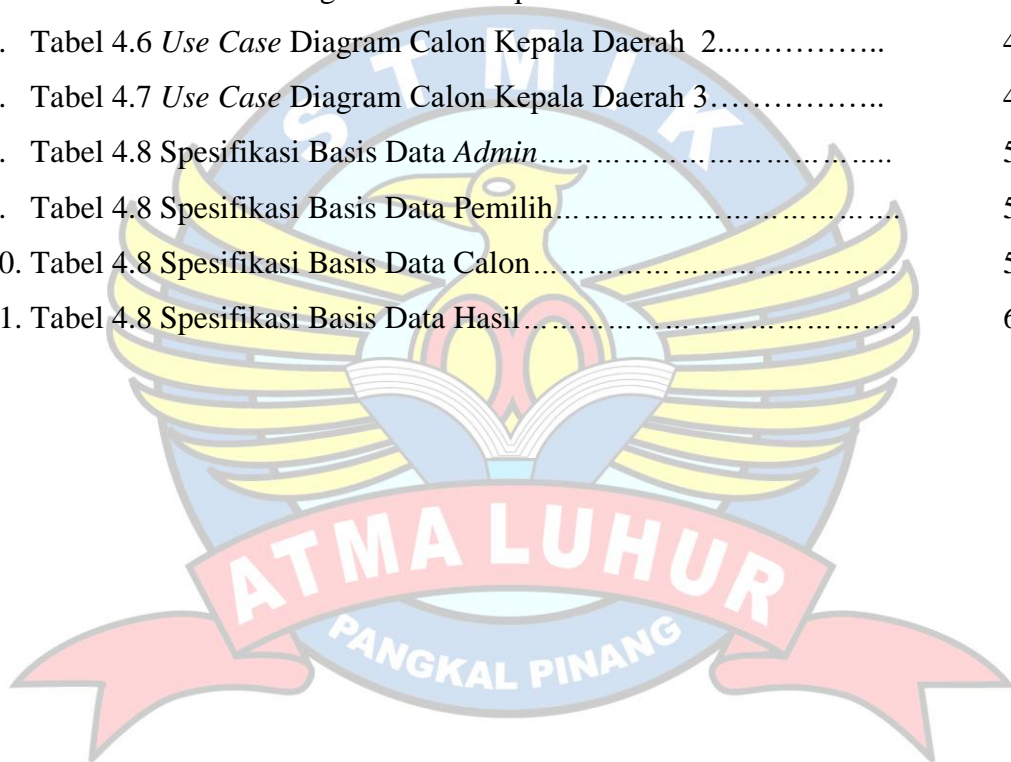
	Halaman
Gambar 2.1. Diagram Komponen Arsitektur Android.....	11
Gambar 2.2 Konsep kriptografi kunci publik RSA.....	15
Gambar 2.3 Tahap-Tahap <i>waterfall</i> .....	21
Gambar 2.4 Simbol – Simbol <i>Use case</i> .....	25
Gambar 2.5 Simbol-Simbol <i>Activity Diagram</i> .....	26
Gambar 2.6 Simbol-Simbol <i>Sequence Diagram</i> .....	27
Gambar 2.7 <i>Class Diagram</i> .....	28
Gambar 4.1 <i>Activity Diagram</i> Sistem Berjalan.....	39
Gambar 4.2 <i>Use Case Diagram</i> Pemilihan.....	41
Gambar 4.3 <i>Activity Diagram</i> Login.....	45
Gambar 4.4 <i>Activity Diagram</i> Pemilihan.....	46
Gambar 4.5 <i>Activity Diagram</i> Hasil.....	47
Gambar 4.6 <i>Activity Diagram</i> Logout.....	48
Gambar 4.7 <i>Activity Diagram</i> Calon Kepala Daerah 1.....	49
Gambar 4.8 <i>Activity Diagram</i> Calon Kepala Daerah 2.....	49
Gambar 4.9 <i>Activity Diagram</i> Calon Kepala Daerah 3.....	50
Gambar 4.10 <i>Sequence Diagram</i> Login.....	51
Gambar 4.11 <i>Sequence Diagram</i> Pemilihan.....	52
Gambar 4.12 <i>Sequence Diagram</i> Hasil.....	53
Gambar 4.13 <i>Sequence Diagram</i> Logout.....	54
Gambar 4.14 <i>Sequence Diagram</i> Calon Kepala Daerah 1.....	55
Gambar 4.15 <i>Sequence Diagram</i> Calon Kepala Daerah 2.....	56
Gambar 4.16 <i>Sequence Diagram</i> Calon Kepala Daerah 3.....	57
Gambar 4.17 <i>Class Diagram</i> .....	58
Gambar 4.18 Halaman Awal.....	61
Gambar 4.19 Halaman Login.....	61
Gambar 4.20 Halaman Menu .....	62
Gambar 4.21 Halaman Pemilihan.....	63

Gambar 4.22 Halaman Calon Kepala Daerah 1.....	64
Gambar 4.23 Halaman Calon Kepala Daerah 2.....	64
Gambar 4.24 Halaman Calon Kepala Daerah 3.....	65
Gambar 4.25 Tampilan Hasil.....	66
Gambar 4.26 Tampilan Awal.....	67
Gambar 4.27 Tampilan <i>Login</i> .....	68
Gambar 4.28 Tampilan Menu.....	69
Gambar 4.29 Tampilan Hasil.....	70
Gambar 4.30 Tampilan Pemilihan.....	71
Gambar 4.31 Tampilan Calon Kepala Daerah 1.....	72
Gambar 4.32 Tampilan Calon Kepala Daerah 2.....	73
Gambar 4.33 Tampilan Calon Kepala Daerah 3.....	74
Gambar 4.34 Tampilan Diagram Algoritma RSA.....	75
Gambar 4.35 Pengujian Wireshark.....	77



## DAFTAR TABEL

	Halaman
1. Tabel 4.1 <i>Use Case Login</i> .....	41
2. Tabel 4.2 <i>Use Case Pemilihan</i> .....	42
3. Tabel 4.3 <i>Use Case Hasil</i> .....	42
4. Tabel 4.4 <i>Use Case Logout</i> .....	43
5. Tabel 4. <i>Use Case Diagram Calon Kepala Daerah 1</i> .....	43
6. Tabel 4.6 <i>Use Case Diagram Calon Kepala Daerah 2</i> .....	44
7. Tabel 4.7 <i>Use Case Diagram Calon Kepala Daerah 3</i> .....	44
8. Tabel 4.8 Spesifikasi Basis Data <i>Admin</i> .....	59
9. Tabel 4.8 Spesifikasi Basis Data <i>Pemilih</i> .....	59
10. Tabel 4.8 Spesifikasi Basis Data <i>Calon</i> .....	59
11. Tabel 4.8 Spesifikasi Basis Data <i>Hasil</i> .....	60





## DAFTAR SIMBOL

### 1. Activity Diagram



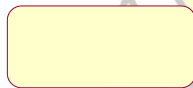
#### *Start Point*

Menggambarkan awal dari suatu aktivitas yang berjalan pada sistem.



#### *End Point*

Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.



#### *Activity State*

Menggambarkan suatu proses / kegiatan bisnis.



NewSwimlane

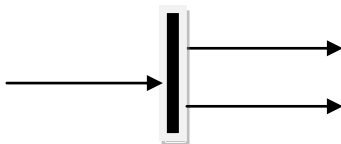
#### *Swimlane*

Menggambarkan pembagian / pengelompokkan berdasarkan tugas dan fungsi sendiri.



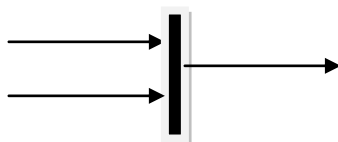
#### *Decision Points*

Menggambarkan pilihan untuk pengambilan keputusan, *true* atau *false*.



#### *Fork*

Menggambarkan aktivitas yang dimulai dengan sebuah aktivitas dan diikuti oleh dua atau lebih aktivitas yang harus dikerjakan.



#### *Join*

Menggambarkan aktivitas yang dimulai dengan dua

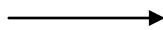
atau lebih aktivitas yang sudah dilakukan dan menghasilkan sebuah aktivitas.

[ ... ]

*Guards*

Sebuah kondisi benar sewaktu melewati sebuah transisi, harus konsisten dan tidak *overlap*.

*Transition*



Menggambarkan aliran perpindahan *control* antara *state*.

## 2. Use Case Diagram



<< include >>

----->

Asosiasi yang termasuk di dalam *use case* lain, yang bersifat harus dilakukan bila *use case* lain tersebut dilakukan.

<< extend >>

----->

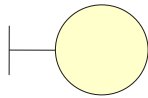
Perluasan dari *use case* lain jika kondisi atau syarat terpenuhi dan tidak harus dilakukan.

### 3. Sequence Diagram



#### *Actor*

Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan sistem.



#### *Boundary*

Sebuah obyek yang menjadi penghubung antara *user* dengan sistem. Contohnya *window*, *dialogue box* atau *screen*(tampilan layar).



#### *Control*

Suatu obyek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas.



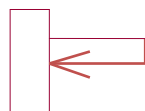
#### *Entity*

Menggambarkan suatu objek yang berisi informasi kegiatan yang terkait yang tetap dan disimpan kedalam suatu *database*.



#### *Object Message*

Menggambarkan pengiriman pesan dari sebuah objek ke objek lain.



#### *Recursive*

Sebuah obyek yang mempunyai sebuah operation kepada dirinya sendiri.



### *Return Message*

Menggambarkan pesan/hubungan antar objek, yang menunjukkan urutan kejadian yang terjadi.



### *Lifeline*

Garis titik-titik yang terhubung dengan obyek, sepanjang *lifeline* terdapat *activation*.

### *Activation*

Activation mewakili sebuah eksekusi operasi dari obyek, panjang kotak ini berbanding dengan durasi aktivasi sebuah operasi.

