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

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
AHMAD RAMADHANI
1411500040

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

LEMBARAN PERYATAAN

Yang bertanda tangan di bawah ini:

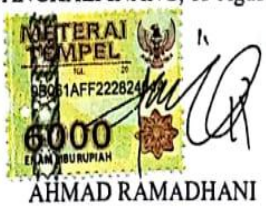
NIM : 1411500040

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 MENGGUNAKAN ALGORITMA RSA BERBASIS ANDROID.

Yang dipersiapkan dan disusun oleh

AHMAD RAMADHANI
1411500040

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 20 Agustus 2018

Anggota	**Dosen Pembimbing**
Eza Budi Perkasa, M.Kom	**Dwi Yuny Sylfania, M.Kom**
NIDN. 0201089201	**NIDN. 0207069301**

Kaprodi Teknik Informatika	**Ketua**
R. Burham Isnanto F., S.Si, M.Kom	**Yohanes Setiawan, M.Kom**
NIDN. 0224048003	**NIDN. 0219068501**

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

KETUA STMIK 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 Buy in terms of the security of the data has not been established althought 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 mengunakan transfortasi 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 menggunaan 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

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR SIMBOL

1. *Activity Diagram*

Start Point

Mengambarkan awal dari suatu aktivitas yang berjalan pada sistem.

End Point

Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.

Activity State

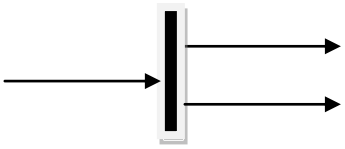
Menggambarkan suatu proses / kegiatan bisnis.

Swimlane

Menggambarkan pembagian / pengelompokkan berdasarkan tugas dan fungsi sendiri.

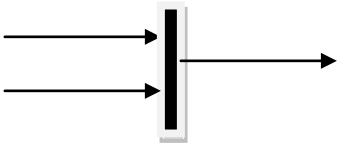
Decision Points

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

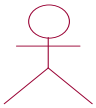
Menggambarkan aktivitas yang dimulai dengan dua

	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*

	*Actor* Abstraksi dari orang atau sistem yang mengaktifkan fungsi dari *use case*.
	*Use Case* Menggambarkan proses sistem dari perpektif pengguna (*user*).
	Relasi/Asosiasi Menggambarkan hubungan antara *actor* dengan *use case*.
<< include >> ---------->	Assosiasi 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.

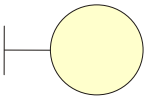
3. *Squence Diagram*



Actor

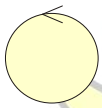
Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan sistem.

.



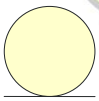
Boundary

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



Control

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

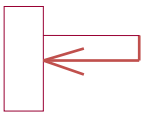


Entity

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 menunjukan 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.