

**PENERAPAN ALGORITMA RSA
UNTUK KEAMANAN PENGIRIMAN DATA
PADA APLIKASI E-VOTING PEMILIHAN KETUA BEM
BERBASIS ANDROID :
STUDI KASUS STMIK ATMA LUHUR PANGKALPINANG**

TESIS



Oleh :

**FRANSISKUS PANCA JUNIAWAN
1311601593**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2016**

**PENERAPAN ALGORITMA RSA
UNTUK KEAMANAN PENGIRIMAN DATA
PADA APLIKASI E-VOTING PEMILIHAN KETUA BEM
BERBASIS ANDROID :
STUDI KASUS STMIK ATMA LUHUR PANGKALPINANG**

TESIS

**Diajukan sebagai salah satu persyaratan
Memperoleh gelar Magister Ilmu Komputer (MKOM)**



Oleh :

**FRANSISKUS PANCA JUNIAWAN
1311601593**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2016**



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Nama Mahasiswa : FRANSISKUS PANCA JUNIAWAN
Nomor Induk Mahasiswa : 1311601593
Program Studi : MAGISTER ILMU KOMPUTER
Konsentrasi : REKAYASA KOMPUTASI TERAPAN
Fakultas/Program : PASCASARJANA

Menyatakan bahwa TESIS yang berjudul :
PENERAPAN ALGORITMA RSA UNTUK KEAMANAN PENGIRIMAN
DATA PADA APLIKASI E-VOTING BERBASIS ANDROID :
STUDI KASUS SIMIK ATMA LUHUR PANGKALPINANG

1. Merupakan hasil karya tulis ilmiah sendiri bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, ... Februari 2016



(FRANSISKUS PJ...)



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Fransiskus Panca Juniawan
Nomor Induk Mahasiswa : 1311601593
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Pasca Sarjana
Judul : Penerapan Algoritma RSA Untuk Keamanan Pengiriman Data Pada Aplikasi E-voting Pemilihan Ketua BEM Berbasis Android: Studi Kasus STMIK Atma Luhur Pangkalpinang

Jakarta, Februari 2016

Tim Penguji:
Ketua,

(Prof. Dr. Moedjiono, M.Sc)

Anggota,

(Dr. Ir. Nazori AZ, M.T)

Pembimbing Utama,

(Mardi Hardjianto, M.Kom)

Pembimbing Pendamping,

(Dr. Ir. Nazori AZ, M.T)

Tanda Tangan:

Ketua Program Studi

(Dr. Ir. Nazori AZ, M.T)

ABSTRAK

Voting merupakan proses pemungutan suara yang dilakukan dalam hal kepemimpinan. Pada umumnya, saat ini *voting* masih menggunakan cara konvensional yang kurang efektif dari segi biaya, tata kelola, dan waktu pengerjaan. Kemungkinan terjadinya kesalahan perhitungan dan kecurangan dalam proses pemilihan juga dapat terjadi. STMIK Atma Luhur masih menggunakan metode *voting* konvensional dalam pemilihan ketua/wakil ketua BEM. Dengan berkembangnya teknologi saat ini, dapat dibuat sistem *e-voting* berbasis *android* guna mengatasi permasalahan *voting* konvensional. Terdapat empat hal sebagai syarat *e-voting* yang dipercaya yaitu *accuracy*, *democracy*, *privacy*, dan *verifiability*. Keamanan *e-voting* menjadi hal mendasar yang harus diperhatikan. Metode kriptografi RSA dapat menjadi solusi dalam menjamin keamanan dalam *e-voting*. Algoritma ini merupakan kriptografi asimetri untuk mengenkripsi dan mendekripsi data dengan kunci yang berbeda. Algoritma RSA dipilih karena memiliki kelebihan berupa tingkat kesulitan dalam memfaktorkan bilangan menjadi bilangan prima. Semakin sulit pemfaktoran bilangan maka semakin sulit pula enkripsi data rahasia ini dipecahkan. Kelebihan lainnya ada pada bentuk keamanan yang lebih tinggi dibanding algoritma simetris, algoritma ini juga tahan terhadap berbagai bentuk serangan, seperti *brute force*. Perancangan sistem *e-voting* berbasis *android* dengan metode analisis dan perancangan berorientasi objek menggunakan *unified modelling language* (UML). Pengujian keamanan sistem menggunakan tool *Wireshark*, dan pengujian validasi menggunakan Pengujian *Black Box*. Untuk pengujian kualitas menggunakan ISO 9126 berdasarkan empat karakteristik kualitas perangkat lunak, yaitu : *functionality*, *reliability*, *usability*, dan *efficiency*. Hasilnya adalah terbentuknya sistem *e-voting* berbasis *android* yang aman, rahasia, dan memenuhi persyaratan *e-voting* yang baik sehingga mahasiswa dapat melakukan *voting* dengan cepat, kapanpun, dan dimanapun.

Kata Kunci : *E-Voting*, RSA, Kriptografi, *Mobile*, *Android*, ISO 9126.

ABSTRACT

Voting is a process that is done in terms of leadership. In case, voting still use conventional methods which are less effective in terms of cost, governance, and working time. The possibility of calculation errors and fraud in the calculation process can also occur. STMIK Atma Luhur still use the conventional voting method in the election of the president / vice president of BEM. With the development of today's technology, we can make electronic voting system based on Android to solve the problems of conventional voting. There are four terms as a condition of e-voting such as accuracy, democracy, privacy, and verifiability. Security of e-voting becomes fundamental things that must be considered. RSA cryptographic methods can be a solution to ensure the security of e-voting. This is an asymmetric cryptographic algorithm to encrypt and decrypt data with different keys. RSA algorithm chosen because it has the advantage of degree of difficulty in factoring numbers into prime numbers. It is increasingly difficult factoring numbers are also encryption of confidential data be solved. Another advantage is in the form of higher security than symmetric algorithm. This algorithm is also resistant to various forms of attack, such as brute force. The design of the e-voting system based on Android with the method of object-oriented analysis and design using the unified modelling language (UML). System security testing using Wireshark, and validation testing using Black Box testing. For quality testing using ISO 9126 that based on four characteristic of software quality, namely: functionality, reliability, usability, and efficiency. The result is the establishment of an e-voting system based on Android that is safe, confidential, and fill the requirements of good e-voting, so the students can do the voting quickly, whenever and wherever.

Keywords : E-voting, RSA algorithm, Cryptography, Mobile, Android, ISO 9126.

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya penulis dapat menyelesaikan penelitian tesis ini. Tujuan dari penulisan penelitian tesis ini adalah sebagai salah satu syarat untuk menyelesaikan Program Studi Magister Ilmu Komputer, Universitas Budi Luhur Jakarta.

Dengan segala kerendahan hati, ucapan terima kasih penulis persembahkan kepada semua pihak yang telah membantu penulis dalam menyusun penelitian tesis ini:

1. Tuhan Yang Maha Esa yang telah memberikan kekuatan dan ketekunan untuk menyelesaikan laporan tesis ini.
2. Orangtua dan keluarga tercinta yang selalu memberikan dukungan dan doa dalam menyelesaikan laporan tesis ini.
3. Bapak Prof. Dr. Moedjiono, M.Sc selaku Direktur Program Pasca Sarjana Universitas Budi Luhur.
4. Bapak Dr. Ir. Nazori A.Z, M. T selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
5. Bapak Mardi Hardjianto, M. Kom dan Bapak Dr. Ir. Nazori AZ, M.T, selaku dosen pembimbing tesis yang telah membimbing dan memotivasi penulis dalam mengerjakan penelitian tesis ini.
6. Rekan-rekan mahasiswa MKOM Universitas Budi Luhur kelas XC Semester 1 dan 2 dan MKOM Semester 3 kelas TI konsentrasi Rekayasa Komputasi Terapan, terima kasih atas kebersamaan, kerja keras dan dukungan semangatnya.
7. Bapak dan Ibu Dosen Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang telah dengan sabar memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar.
8. Teman-teman perkuliahan terbaik Hengki, Rendy Rian Chrisna Putra, Laurentinus, Chandra Kirana, dan adik-adik junior yang sangat unik. Terimakasih untuk 2 tahun perkuliahan yang dijalani bersama. Terimakasih karena memberikan warna di kehidupan penulis. Terimakasih karena selalu berada di samping penulis. Terimakasih karena telah bersedia mengikuti roda kehidupan penulis tanpa mengeluh. Terimakasih karena telah menjadi keluarga, sahabat, dan teman di tanah rantau Jakarta. Terimakasih untuk semuanya.

Penulis menyadari bahwa laporan penelitian tesis ini masih jauh dari sempurna. Karena itu, penulis dengan senang hati menerima kritik dan saran yang membangun. Semoga penelitian tesis ini dapat memberikan manfaat semaksimal mungkin.

Jakarta, 13 Januari 2016

Fransiskus Panca Juniawan

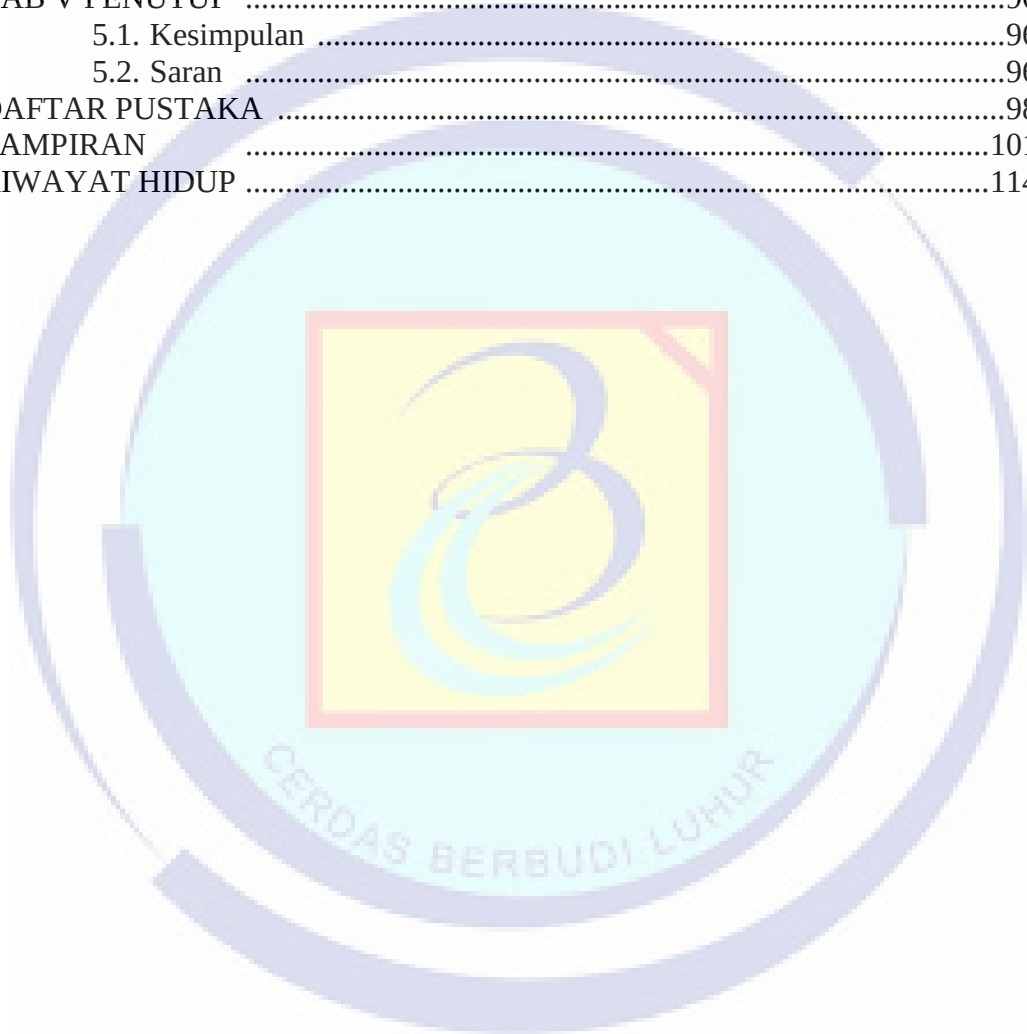


DAFTAR ISI

	Halaman
ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian	2
1.2.1. Identifikasi Masalah	2
1.2.2. Pembatasan Masalah	3
1.2.3. Rumusan Masalah	3
1.3. Tujuan dan Manfaat Penelitian	3
1.3.1. Tujuan Penelitian	3
1.3.2. Manfaat Penelitian	3
1.4. Tata Urut Penulisan	4
1.5. Daftar Pengertian	5
BAB II LANDASAN TEORI DAN KERANGKA KONSEP	7
2.1 Tinjauan Pustaka	7
2.1.1 E-Voting	7
2.1.2 Kriptografi	10
2.1.3 Algoritma Kriptografi RSA	13
2.1.4 Unified Modelling Language (UML)	19
2.1.5 Pengujian Black Box	21
2.1.6 ISO 9126	22
2.2 Tinjauan Studi	26
2.3 Tinjauan Objek Penelitian	36
2.3.1 Sejarah Singkat STMIK Atma Luhur	36
2.3.2 Struktur Organisasi	37
2.3.3 Visi dan Misi Organisasi	38
2.4 Kerangka Konsep	39
2.5 Hipotesis	40
BAB III METODE DAN RANCANGAN PENELITIAN	41
3.1 Metode Penelitian	41
3.2 Metode Pengumpulan Sampel	41
3.3 Metode Pengumpulan Data	41
3.4 Instrument Penelitian	42
3.4.1 Instrument Pengumpulan Data	42
3.4.2 Instrument Pengujian Data	42
3.5 Teknik Analisis, Rancangan, dan Pengujian Data	43
3.5.1 Teknik Analisis	43

3.5.2 Teknik Perancangan	43
3.5.3 Teknik Pengujian	44
3.5.3.1 Pengujian Validasi dengan <i>Black Box</i>	45
3.5.3.2 Pengujian Kualitas dengan ISO 9126	45
3.5.3.2.1 <i>Instrument</i> Pengujian	45
3.5.3.2.2 Pengujian Validitas <i>Instrument</i>	47
3.5.3.2.3 Pengujian Reliabilitas <i>Instrument</i>	47
3.5.3.2.4 Pengolahan Data Pengujian	48
3.6 Langkah-Langkah Penelitian	49
3.7 Jadwal Penelitian	51
BAB IV PEMBAHASAN HASIL PENELITIAN	53
4.1. Analisa Proses Pengiriman Data	53
4.2. Analisa Proses Enkripsi Dekripsi Data	54
4.3. Analisa Kebutuhan dan Non Fungsional	59
4.3.1. Analisa Kebutuhan Fungsional	59
4.3.2. Analisa Kebutuhan Non Fungsional	59
4.4. Arsitektur Sistem	60
4.5. Analisa dan Perancangan Sistem	62
4.5.1. Use Case Diagram	62
4.5.2. Class Diagram	64
4.5.3. Activity Diagram	65
4.5.4. Sequence Diagram	68
4.5.5. Konstruksi Database	73
4.6. Implementasi Sistem	74
4.6.1. Spesifikasi Perangkat Keras	75
4.6.2. Spesifikasi Perangkat Lunak	75
4.6.3. Hasil Implementasi Sistem	75
4.6.3.1. Tampilan Awal	75
4.6.3.2. Tampilan Halaman Menu	76
4.6.3.3. Tampilan Halaman Login	76
4.6.3.4. Tampilan Halaman Menu Pemilih	77
4.6.3.5. Tampilan Halaman Kandidat	77
4.6.3.6. Tampilan Halaman Visi Misi dan Voting Calon ...	78
4.6.3.7. Tampilan Halaman Sukses Voting	79
4.6.3.8. Tampilan Halaman Hasil	80
4.7. Pengujian Sistem	80
4.7.1. Lingkungan Pengujian	80
4.7.1.1. Hardware	81
4.7.1.2. Software	81
4.7.2. Pengujian Keamanan	81
4.7.2.1.. Pembuktian Dengan LogCat Eclipse	81
4.7.2.2.. Pengujian Keamanan Dengan Wireshark	84
4.7.3. Pengujian Validasi	87
4.7.4. Pengujian Kualitas	88
4.7.4.1.. Karakteristik Responden	88
4.7.4.2.. Uji ISO 9126	88

4.7.4.3.. Kesimpulan Hasil Pengujian dan Pembuktian	
Hipotesis	93
4.8. Implikasi Penelitian	93
4.8.1. Aspek Sistem ..	93
4.8.2. Aspek Manajerial	94
4.8.3. Aspek Penelitian lanjut	94
4.9. Rencana Implementasi Sistem	94
BAB V PENUTUP	96
5.1. Kesimpulan	96
5.2. Saran	96
DAFTAR PUSTAKA	98
LAMPIRAN	101
RIWAYAT HIDUP	114



DAFTAR GAMBAR

Gambar	Halaman
II-1 Bagan Algoritma Kriptografi	11
II-2 Kriptografi Kunci Simetris	12
II-3 Kriptografi Kunci Asimetris	13
II-4 Flowchart Enkripsi RSA	15
II-5 Flowchart Dekripsi RSA	16
II-6 Simbol <i>Use Case Diagram</i>	20
II-7 Simbol <i>Class Diagram</i>	20
II-8 Simbol <i>Sequence Diagram</i>	21
II-9 Simbol <i>Activity Diagram</i>	21
II-10 Struktur Organisasi Yayasan Atma Luhur	37
II-11 Struktur Organisasi STMIK Atma Luhur	38
II-12 Kerangka Konsep Penelitian	39
III-1 Tahapan Perancangan Sistem	44
III-2 Langkah-Langkah Penelitian	49
IV-1 Proses Pengiriman Data Pada Aplikasi	53
IV-2 Proses Enkripsi	54
IV-3 Proses Dekripsi	55
IV-4 Arsitektur Sistem Voting Berbasis Android	60
IV-5 Arsitektur Sistem Sisi Software dan Hardware	61
IV-6 Use Case Diagram Pemilih/User	62
IV-7 Class Diagram	65
IV-8 Activity Diagram Login	65
IV-9 Activity Diagram Visi Misi	66
IV-10 Activity Diagram Voting/Pemilihan	66
IV-11 Activity Diagram Hasil Oleh Pemilih	67
IV-12 Activity Diagram Hasil Oleh User	67
IV-13 Activity Diagram Logout	68
IV-14 Sequence Diagram Login	69
IV-15 Sequence Diagram Visi Misi	70
IV-16 Sequence Diagram Voting/Pemilihan	70
IV-17 Sequence Diagram Hasil Oleh Pemilih	71
IV-18 Sequence Diagram Hasil Oleh User	72
IV-19 Sequence Diagram Logout	73
IV-20 Entitas Tabel Calon	74
IV-21 Entitas Tabel Mahasiswa	74
IV-22 Entitas Tabel Rincian	74
IV-23 Tampilan Utama Aplikasi	76
IV-24 Tampilan Menu	76
IV-25 Tampilan Menu Login	77
IV-26 Tampilan Halaman Menu Pemilih	77
IV-27 Tampilan Kandidat	78
IV-28 Tampilan Halaman Visi Misi dan Voting Calon	79

IV-29 Tampilan Voting Sukses	79
IV-30 Tampilan Hasil Voting	80
IV-31 Proses Login	82
IV-32 Pemilihan Bilangan Prima Acak	82
IV-33 Input NIM	82
IV-34 Sukses Voting	82
IV-35 Tampilan LogCat Eclipse	84
IV-36 Arsitektur Pengujian Keamanan	84
IV-37 Hasil Pengujian Wireshark Tanpa Enkripsi	85
IV-38 Hasil Pengujian Wireshark Dengan Enkripsi	86
IV-39 Data Enkripsi Lengkap	86



DAFTAR TABEL

Tabel	Halaman
II-1 Contoh Perhitungan Pencarian FPB	17
II-2 Contoh Perhitungan Pencarian Nilai d	17
II-3 Contoh Enkripsi Algoritma RSA	18
II-4 Contoh Dekripsi Algoritma RSA	19
II-5 Karakteristik Kualitas Model ISO 9126	24
II-6 Tinjauan Studi	31
III-1 Skala Pengukuran	45
III-2 Kisi-kisi Pengukuran Kualitas Perangkat Lunak dan Indikator	46
III-3 Kriteria Presentase Tanggapan Responden	48
III-4 Jadwal Penelitian	50
IV-1 Pencarian Nilai e	56
IV-2 Pencarian Nilai k	57
IV-3 Perhitungan Enkripsi Data	58
IV-4 Perhitungan Dekripsi Data	58
IV-5 Software yang Digunakan	61
IV-6 Penjelasan Aktor	63
IV-7 Penjabaran Use Case	63
IV-8 Hasil Pengujian Validasi	87
IV-9 Karakteristik Responden Mahasiswa	88
IV-10 Tanggapan Responden Aspek Functionality	89
IV-11 Tanggapan Responden Aspek Reliability	90
IV-12 Tanggapan Responden Aspek Usability	91
IV-13 Tanggapan Responden Aspek Efficiency	92
IV-14 Tingkat Kualitas Perangkat Lunak Keseluruhan	92
IV-15 Rencana Implementasi Sistem	95

DAFTAR LAMPIRAN

Lampiran	Halaman
1. Contoh Hasil Kuesioner Uji Kualitas Model ISO 9126.....	101
2. Rekapitulasi Skor Data Mentah Hasil Kuesioner ISO 9126	104
3. Contoh Source Code Aplikasi	109



DAFTAR PUSTAKA

- [Adnan 2014] Adnan, 2014. Kinerja Tanda Tangan Digital RSA 1024 bit pada Simulasi E-Voting Menggunakan Prosesor Multicore. *Seminar Nasional Aplikasi Teknologi Informasi*.
- [Afrin 2013] Afrin, T. & Satao, K., 2013. Detailed Implementation of E-Voting System for on Duty Persons using RSA Algorithm with Kerberos Concept. *International Journal of Innovative Research in Computer and Communication Engineering*, 1(7).
- [Agustina 2009] Agustina, E.R. & Kurniati, A., 2009. Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada e-Voting di Indonesia. *Seminar Nasional Informatika UPN*, pp.22–28.
- [Al-Anie 2011] Al-Anie, H.K., Alia, M.A. & Hnaif, A.A., 2011. E-Voting Protocol Based on Public-Key Cryptography. *International Journal of Network Security & Its Application*, 3(4).
- [Alfred 1997] Alfred, J.M., Paul, C.O. & Scott, A. V., 1997. *Handbook of Applied Cryptography*, Florida: CRC Press LLC.
- [Amsyah 2005] Amsyah, Z., 2005. *Manajemen Sistem Informasi* 5th ed., Jakarta: PT. Gramedia Pustaka Utama.
- [Arriyus 2008] Ariyus, D., 2008. *Pengantar Ilmu Kriptografi* 1st ed., Yogyakarta: Andi.
- [Autade 2012] Autade, K. et al., 2012. E-voting on Android System. , 2(2).
- [Boneh 1999] Boneh, D., 1999. *Twenty Years of Attacks on the RSA Cryptosystem*,
- [Ebrahim 2013] Ebrahim et al., 2013. Symmetric Algortihm Survey: A Comparative Analysis. *International Journal of Computer Applications*, 61(20).
- [Europe 2005] Europe, C. of, 2005. *Legal, Operational and Technical Standards for E-Voting*, Canada: Council of Europe Publishing.
- [Farid 2014] Farid, R.B.I., 2014. *Prototipe CRM Perguruan Tinggi Untuk Meningkatkan Daya Saing*. Budi Luhur.