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: Tanda Tangan:
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) .....

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 solustion to ensure the security of e-voting. This is an asymmetric cryptographic algroithme to encrypt and decrypt data with different keys. RSA algorithm choses 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 confidentioal 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 whereever.

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

DAFTAR GAMBAR

Gambar Halaman

DAFTAR TABEL

DAFTAR LAMPIRAN

Lampiran Halaman

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.