MODEL MODIFIKASI KRIPTOGRAFI ALGORITMA RSAUNTUK KEAMANAN DATA PADA DATABASE E-VOTING

TESIS

Oleh:

MARTONO

1311601775

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

MODEL MODIFIKASI KRIPTOGRAFI ALGORITMA RSA UNTUK KEAMANAN DATA PADA DATABASE E-VOTING

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)

Oleh:
MARTONO
1311601775

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

JAKARTA
2015

PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa	: Martono
Nomor Induk Mahasiswa	: 1311601775
Program Studi	: Magister Ilmu Komputer
Konsentrasi	: Rekayasa Komputasi Terapan
Fakultas/Program	: Pascasarjana

Menyatakan bahwa tesis yang berjudul :
Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijinkan 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, 18 September 2015

(Martono)

PROGRAM STUDI: MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Martono
Nomor Induk Mahasiswa : 1311601775
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul : Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting

Jakarta, 18 September 2015

Tim Penguji : Tanda Tangan :

Ketua,
Dr. Moedjiono, M.Sc .....

Anggota,
Ir. Wendi Usino, MM, M.Sc, PhD .....

Pembimbing,
Dr. Ir. Nazori AZ, MT .....

Ketua Program Studi

Dr. Ir. Nazori AZ, MT

ABSTRAK

Masalah keamanan komputer merupakan sesuatu yang sangat penting. Keamanan merupakan bentuk tindakan untuk mempertahankan sesuatu hal dari berbagai macam gangguan dan ancaman. Keamanan komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga dari keamanan datanya.Keamanan data sangat dibutuhkan agar data tidak jatuh ke tangan orang yang tidak berhak atas data tersebut dan untuk menghindari perubahan data tersebut oleh pihak lain.Salah satu cara untuk mengamankan data adalah dengan menggunakan kriptografi.Kriptografi merupakan ilmu dan sekaligus seni untuk mengamankan data yang didalamnyaterdapat algoritma tertentu yang bertujuan sebagai confusion atau pembingungan, dengan cara mengubah teks polos (plaintext) menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia (ciphertext).Proses mengubah dari plaintext menjadi ciphertext disebut enkripsi sedangkan proses mengubah dari ciphertext menjadi plaintext disebut dekripsi. Sudah banyakdikembangkan algoritma kriptografi. Semakin rumit algoritma kriptografinya, semakin sulit pula ciphertext dapat di baca artinya (kerahasiaan lebih terjamin). Algoritma kriptografi yang digunakan dalam penelitian ini adalah algoritma RSA dengan pengembangan atau modifikasi. Algoritma RSA termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key). Sampai saat ini, algoritma kriptografi RSA merupakan salah satu algoritma yang paling maju dalam bidang kriptografi dan banyak digunakan karena kehandalannya.Dalam tesis ini membahas tentang model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-votingdan metode penelitian yang digunakan adalah metode penelitian eksperimen serta metode pengujian sistem yang digunakan adalah metode black box untuk pengujian validasi dan metode eksperimen untuk pengujian kualitas.Hasil dari penelitian tersebut dapat membantu menjaga dan meningkatkan kerahasiaan dan keamanan data pada databaseterutama database e-voting, sehingga data pada database tersebut tidak akan dapat terbaca secara langsung (karena telah dienkripsi) tanpa melalui proses dekripsi.

Kata Kunci : Keamanan Komputer, Keamanan Data, Kriptografi, Plaintext, Ciphertext, Enkripsi, Dekripsi, Algoritma RSA, Kunci Publik (Public Key), Kunci Pribadi (Private Key).

ABSTRACT

Computer security problem is a very important thing. Security is an action to defend something from any destruction and threat. Computer security not only focus on computer equipment but also focus on data security. Data security is needed for protect the data from the other people who doesn't has authority and avoid data transformation by other people. One of the method to protect data is using cryptography. Cryptography is a knowledge and also an art to protect data which is has a specific algorithm to intend as confusion, by change the plaintext into a text that can't be read the meaning by other people directly (ciphertext). The changing process from plaintext to ciphertext is called encryption whereas the changing process from ciphertext to plaintext is called decryption. It's already a lot cryptography algorithm development. The more complex it's cryptography algorithm, make it (ciphertext) more difficult to read the meaning (the confidentiality more guaranted). Cryptography algorithm that used in this research is RSA algorithm with development or modification. The RSA algorithm is include in asymmetric cryptography algorithm that have two keys, i.e. public key and private key. Until now RSA cryptography algorithm is one of the most advanced algorithm in cryptography and most used because it's reliability. This graduate thesis discuss about RSA cryptography algorithm modification model for data security at e-voting database and the research method that used is experiment research method and system examination method that used is black box method for validation examination and experiment method for quality examination. The result from this research to help user protect their data and improve confidential and data security especially e-voting database, so the data at database can't be read directly (because already encrypted) without decryption process.

Keywords : *Computer Security, Data Security, Cryptography, Plaintext, Ciphertext, Encryption, Decryption, RSA Algorithm, Public Key, Private Key.*

KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadirat Tuhan Yang Maha Esa, karena berkat rahmat dan karunianya penulis dapat menyelesaikan tesis yang berjudul "Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting" sebagai salah satu syarat untuk memperoleh gelar MagisterIlmu Komputer pada Universitas Budi Luhur. Pada kesempatan ini penulis mengucapkan terima kasih kepada :

1. Bapak Dr. Moedjiono, M.Sc selaku Direktur Program Pascasarjana Universitas Budi Luhur.
2. Bapak Dr. Ir. Nazori AZ, MT selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku Pembimbing Tesis.
3. Bapak Ir. Eddy Anthony, SH, MM selaku Ketua Yayasan Dinamika Bangsa Jambi dimana tempat penulis bekerja.
4. Bapak Dr. Ir. Herry Mulyono, MM selaku Pengurus Harian Yayasan Dinamika Bangsa Jambi dimana tempat penulis bekerja.
5. Seluruh Dosen Universitas Budi Luhur yang telah memberikan pengetahuan dan pengarahan selama penulis mengikuti pendidikan di Universitas Budi Luhur.
6. Seluruh pihak yang telah membantu baik secara langsung maupun tidak langsung hingga terselesaikannya tesis ini.

Penulis menyadari bahwa dalam tesis ini masih banyak kekurangannya, untuk itu penulis mengharapkan kritik dan saran untuk penyempurnaan yang akan datang. Akhir kata penulis mengucapkan terima kasih.

Jakarta, 18 September 2015
Penulis,

Martono

DAFTAR ISI

Halaman

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI iv
DAFTAR GAMBAR vi
DAFTAR TABEL viii
DAFTAR LAMPIRAN ix
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Masalah Penelitian 3
1.2.1 Indentifikasi Masalah 3
1.2.2 Batasan Masalah 4
1.2.3 Rumusan Masalah 4
1.3 Tujuan dan Manfaat Penelitian 4
1.3.1 Tujuan Penelitian 4
1.3.2 Manfaat Penelitian 5
1.4 Sistematika Penulisan 5
1.5 Daftar Pengertian 6
BAB II LANDASAN TEORI DAN KERANGKA KONSEP 8
2.1 Tinjauan Pustaka 8
2.1.1 Kriptografi 8
2.1.2 Algoritma RSA 11
2.1.3 Keamanan Data 15
2.1.4 Database 17
2.1.5 E-Voting 18
2.2 Tinjauan Studi 20
2.3 Tinjauan Objek Penelitian 28
2.4 Kerangka Konsep 29
2.5 Hipotesis 30
BAB III METODOLOGI DAN RANCANGAN PENELITIAN 31
3.1 Metode Penelitian 31
3.2 Metode Pengumpulan Data 31
3.3 Metode Pengujian Sistem 31
3.4 Langkah-Langkah Penelitian 32
3.5 Jadwal Penelitian 34
BAB IV PEMBAHASAN HASIL PENELITIAN 35
4.1 Analisis Sistem 35
4.2 Perancangan Sistem 39
4.2.1 Perancangan Model Modifikasi Kriptografi Algoritma RSA . 40
4.2.2 Perancangan Tampilan Sistem 43
4.3 Implementasi Sistem 60
4.3.1 Spesifikasi Perangkat Keras 60

4.3.2 Spesifikasi Perangkat Lunak 60
4.3.3 Hasil Implementasi Sistem 60
4.4 Pengujian Sistem 79
4.4.1 Pengujian Validasi 80
4.4.2 Pengujian Kualitas 97
4.5 Implikasi Penelitian 101
4.5.1 Aspek Sistem 101
4.5.2 Aspek Manajerial 102
4.5.3 Aspek Penelitian Lanjut 102
4.6 Rencana Implementasi Sistem 102
BAB V PENUTUP 104
5.1 Kesimpulan 104
5.2 Saran 104
DAFTAR PUSTAKA 106
LAMPIRAN 108
RIWAYAT HIDUP SINGKAT 126

DAFTAR GAMBAR

Gambar		Halaman
II-1	Diagram Proses Enkripsi dan Dekripsi	8
II-2	Alur Kriptografi Kunci Simetris	9
II-3	Alur Kriptografi Kunci Asimetris	10
II-4	Alur Enkripsi dan Dekripsi Algoritma RSA Sebelum Dimodifikasi	27
II-5	Alur Enkripsi dan Dekripsi Algoritma RSA Sesudah Dimodifikasi	28
II-6	Kerangka Konsep	29
III-1	Langkah-Langkah Penelitian	32
IV-1	Use Case Diagram	35
IV-2	Perancangan Model Modifikasi Kriptografi Algoritma RSA	40
IV-3	Perancangan Tampilan Halaman Utama	44
IV-4	Perancangan Tampilan Halaman Pendaftaran Pemilih	45
IV-5	Perancangan Tampilan Halaman Pengumuman Daftar Pemilih	46
IV-6	Perancangan Tampilan Halaman Pengumuman Capres dan Cawapres	47
IV-7	Perancangan Tampilan Halaman Pengumuman Hasil Perolehan Suara	48
IV-8	Perancangan Tampilan Halaman Pengumuman Pemenang	49
IV-9	Perancangan Tampilan Halaman Ubah Password Administrator	50
IV-10	Perancangan Tampilan Halaman Ubah Password Pemilih	50
IV-11	Perancangan Tampilan Halaman Petunjuk Teks	51
IV-12	Perancangan Tampilan Halaman Petunjuk Video	51
IV-13	Perancangan Tampilan Halaman Login Administrator	52
IV-14	Perancangan Tampilan Halaman Login Pemilih	52
IV-15	Perancangan Tampilan Halaman Home Administrator	53
IV-16	Perancangan Tampilan Halaman Input Data Mahasiswa	53
IV-17	Perancangan Tampilan Halaman Input Data Capres dan Cawapres	54
IV-18	Perancangan Tampilan Halaman Input Data Nomor Urut	54
IV-19	Perancangan Tampilan Halaman Update Data Mahasiswa	55
IV-20	Perancangan Tampilan Halaman Update Data Pemilih	56
IV-21	Perancangan Tampilan Halaman Update Data Capres dan Cawapres	56
IV-22	Perancangan Tampilan Halaman Update Data Nomor Urut	57
IV-23	Perancangan Tampilan Halaman Ubah Status	57
IV-24	Perancangan Tampilan Halaman Edit Data Mahasiswa	58
IV-25	Perancangan Tampilan Halaman Edit Data Capres dan Cawapres	58
IV-26	Perancangan Tampilan Halaman Pemilih	59
IV-27	Implementasi Tampilan Halaman Utama	61
IV-28	Implementasi Tampilan Halaman Pendaftaran Pemilih	62
IV-29	Implementasi Tampilan Halaman Pengumuman Daftar Pemilih	63
IV-30	Implementasi Tampilan Halaman Pengumuman Capres dan Cawapres	64
IV-31	Implementasi Tampilan Halaman Pengumuman Hasil Perolehan Suara	65
IV-32	Implementasi Tampilan Halaman Pengumuman Pemenang	66
IV-33	Implementasi Tampilan Halaman Ubah Password Administrator	67
IV-34	Implementasi Tampilan Halaman Ubah Password Pemilih	67
IV-35	Implementasi Tampilan Halaman Petunjuk Teks	68

IV-36 Implementasi Tampilan Halaman Petunjuk Video 69
IV-37 Implementasi Tampilan Halaman Login Administrator 70
IV-38 Implementasi Tampilan Halaman Login Pemilih 70
IV-39 Implementasi Tampilan Halaman Home Administrator 71
IV-40 Implementasi Tampilan Halaman Input Data Mahasiswa..... 72
IV-41 Implementasi Tampilan Halaman Input Data Capres dan Cawapres..... 72
IV-42 Implementasi Tampilan Halaman Input Data Nomor Urut 73
IV-43 Implementasi Tampilan Halaman Update Data Mahasiswa..... 74
IV-44 Implementasi Tampilan Halaman Update Data Pemilih 75
IV-45 Implementasi Tampilan Halaman Update Data Capres dan Cawapres . 76
IV-46 Implementasi Tampilan Halaman Update Data Nomor Urut 76
IV-47 Implementasi Tampilan Halaman Ubah Status 77
IV-48 Implementasi Tampilan Halaman Edit Data Mahasiswa 77
IV-49 Implementasi Tampilan Halaman Edit Data Capres dan Cawapres 78
IV-50 Implementasi Tampilan Halaman Pemilih 79
IV-51 Modul Pendaftaran Pemilih 95
IV-52 Hasil Yang Didapat Pada Identifikasi 1A 95
IV-53 Hasil Yang Didapat Pada Identifikasi 1B..... 96
IV-54 Hasil Yang Didapat Pada Identifikasi 1C..... 96
IV-55 Grafik Kinerja Untuk Proses Enkripsi.....100
IV-56 Grafik Kinerja Untuk Proses Dekripsi 101

DAFTAR TABEL

Tabel		Halaman
II-1	Hitung Nilai e	12
II-2	Hitung Nilai d	13
II-3	Contoh Proses Enkripsi	13
II-4	Contoh Proses Dekripsi	14
II-5	Tinjauan Studi	23
III-1	Jadwal Penelitian	34
IV-1	Penjelasan Aktor	36
IV-2	Penjelasan Use Case	37
IV-3	Contoh Proses Enkripsi	42
IV-4	Contoh Proses Dekripsi	43
IV-5	Hasil Pengujian Validasi	80
IV-6	Hasil Pengujian Kualitas	98
IV-7	Rencana Implementasi Sistem	103

DAFTAR LAMPIRAN

Lampiran		Halaman
1	Proses Pengujian Kualitas (5 Karakter)	108
2	Proses Pengujian Kualitas (10 Karakter)	110
3	Proses Pengujian Kualitas (50 Karakter)	112
4	Proses Pengujian Kualitas (100 Karakter)	114
5	Proses Pengujian Kualitas (500 Karakter)	116
6	Proses Pengujian Kualitas (1000 Karakter)	118
7	Proses Pengujian Kualitas (5000 Karakter)	120
8	Proses Pengujian Kualitas (10000 Karakter)	123

DAFTAR PUSTAKA

[Amsyah 2005]Zulkifli Amsyah. "Manajemen Sistem Informasi". 5th ed. Jakarta : PT Gramedia Pustaka Utama. 2005.

[Ardana 2010] I Gusti Made Ardana. "Menuju E-Voting". 2010. http://artikel-media.blogspot.com/2010/04/menuju-e-voting.html. (Diakses 10 Mei 2014).

[Arifin 2009] Zainal Arifin. "Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi Yang Aman". *Jurnal Informatika Mulawarman*, Vol.4 No.3, (September, 2009) : 7-14.

[Ariyus 2008] Dony Ariyus. "Pengantar Ilmu Kriptografi". 1th ed. Yogyakarta : Andi. 2008.

[Gutub 2010] Adnan Abdul-Aziz Gutub. "Pixel Indicator Technique for RGB Image Steganography". *Journal of Emerging Technologies in Web Intelligence*, Vol.2 No.1, (Februari, 2010) : 1-9.

[Hartono 2004] Budi Hartono. "Ruang Lingkup Kriptografi Untuk Mengamankan Data". *Jurnal Dinamika Informatika*, Vol.IX No.2, (Mei, 2004) : 1-8.

[Jogiyanto 2005] Jogiyanto HM."Analisis dan Desain". 3th ed. Yogyakarta : Andi. 2005.

[Kristanto 2004] Harianto Kristanto. "Konsep dan Perancangan Database". 3th ed.Yogyakarta : Andi. 2004.

[Lasmana 2014] Indra Lasmana. "Model Implementasi Keamanan Web Service dengan Kriptografi dan Tanda Tangan Digital Pada Sistem Informasi Akademik : Studi Kasus Universitas XYZ". Tesis, Universitas Budi Luhur, 2014.

[Listiyono 2009] Hersatoto Listiyono. "Implementasi Algoritma Kunci Publik Pada Algoritma RSA". *Jurnal Dinamika Informatika*, Vol.I No.2, (September, 2009) : 95-99.

[Lubis 2013] Muhammad Safri Lubis, et.al. "Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email".*Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, (Juni, 2013) : 28-33.

[Munir 2006] Rinaldi Munir. "Pengantar Kriptografi".1th ed. Bandung : Informatika. 2006.