Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data Dengan Bahasa Pemrograman Java Server Pages (JSP)

TESIS

Oleh:
Fuad Lutfi
1111600282

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

JAKARTA
2013

Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data Dengan Bahasa Pemrograman Java Server Pages (JSP)

TESIS

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

Oleh:

Fuad Lutfi

1111600282

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

JAKARTA
2013

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

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa	: Fuad Lutfi
Nomor Induk Mahasiswa	: 1111600282
Program Studi	: Magister Ilmu Komputer
Konsentrasi	: Teknologi Sistem Informasi
Fakultas/Program	: Pasca Sarjana

menyatakan bahwa Tesis yang berjudul:

Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data Dengan Bahasa Pemrograman Java Server Pages (JSP)

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, 22 Agustus 2013

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

LEMBAR PENGESAHAN

Nama Mahasiswa : Fuad Lutfi
Nomor Induk Mahasiswa : 1111600282
Konsentrasi : Teknologi Sistem Informasi
Judul Tesis : Prototipe Sistem Kriptografi Kunci Publik Algoritma Rivest Shamir Adleman (RSA) Untuk Keamanan Pertukaran Data Dengan Bahasa Pemrograman Java Server Pages (JSP)

Jakarta, 22 Agustus 2013

Tim Penguji: Tanda Tangan:

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

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

Pembimbing,
Dr. Ir. Nazori Az, M.T .....

Ketua Program Studi

Dr., Ir. Nazori Az, M.T

ABSTRAK

Pesatnya perkembangan teknologi informasi menggunakan komputer, mengakibatkan semakin bertambah pula masalah yang mengiringi perkembangan teknologi tersebut. Masalah keamanan data merupakan faktor yang harus diperhatikan dalam perkembangan teknologi informasi selanjutnya. Jika membicarakan tentang teknologi informasi tentunya berkaitan pula dengan isi yang terkandung dalam informasi tersebut. Informasi yang akan disampaikan/dikirimkan haruslah sesuai dengan isi yang ingin di informasikan. Pengiriman data dan informasi hendaknya dapat memastikan kemanan dari data dan informasi yang dikirimkannya, sehingga pengiriman informasi dapat dipertanggung jawabkan dari segi kerahasiaan data dan informasi, keaslian data dan informasinya, keutuhan dari data dan informasi yang dikirimkan, dan juga si pengirim data dan informasi tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut. Untuk memenuhi aspek-aspek dan komponen-komponen dalam pengiriman data, dibutuhkan suatu metode pengaman data, algoritma kriptografi Asimetrik Rivest Shamir Adleman. Penelitian ini menggunakan metode pengembangan sistem informasi model *System Development Life Cycle* (SDLC), dengan tahapan yang dilakukan meliputi, perencanaan sistem, analisis sistem, desain sistem secara umum, evaluasi dan seleksi sistem, desain sistem secara terinci, implementasi. Penggunaan kriptografi asimetrik dianggap sebagai metode enkripsi yang paling aman saat ini, dimana digunakan dua kunci yang memiliki fungsi untuk melakukan enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki kunci pribadi untuk melakukan pembongakaran terhadap sandi yang dikirimkan untuknya dengan pasangan kunci publiknya. RSA adalah salah satu algoritma asimetrik yang paling populer digunakan dimana dalam penerapannya kunci pribadi dan kunci publik dapat digunakan secara berlawanan dengan tujuan yang berbeda. Pada penelitian tesis ini penulis melakukan pengujian enkripsi dan dekripsi menggunakan 2 (dua) kekuatan kunci RSA 1024 bits dan 2048 bits dengan menguji keefektifan waktu enkripsi dan dekripsi dari 4 (empat) format file yang berbeda.

Kata Kunci: Kriptografi, Algoritma, RSA, Kunci Publik, Kunci Pribadi, Informasi, Data, Enkripsi, Dekripsi.

ABSTRACT

The rapid development of information technology using a computer, resulting in increasingly also problems that accompany the development of these technologies. A data security issue is a factor that must be considered in the development of information technologies further. If we are talking about information technology course also related to the content contained in such information. The information will be delivered must be in accordance with the content that you want to inform. Delivery of data and information should be able to ensure the security of the data and information it sends, so it can be responsible for the transmission of information in terms of confidentiality of data and information, the authenticity of data and information, the integrity of the data and information submitted, as well as the sender of data and information can not be deny that it was he who sent the information. To meet these aspects and components in the delivery of data, we need a method of data security, asymmetric cryptographic algorithm Rivest Shamir Adleman. This study uses a model of information system development System Development Life Cycle (SDLC), with steps being taken include, system planning, system analysis, system design in general, the evaluation and selection system, detailed system design, implementation. The use of asymmetric cryptography is considered as the most secure encryption methods at this time, which used two keys that have a function to perform the encryption and another for decryption. All those who get public key can use it to encrypt a message, while only one person who has the private key to do pembongakaran the password that was sent to him with a public key pair. RSA is one of the most popular asymmetric algorithms used in the application where the private key and public key can be used as opposed to a different destination. On this thesis study authors tested the encryption and decryption using two (2) power and 1024 bits RSA key 2048 bits to test the effectiveness of time encryption and decryption of 4 (four) different file formats.

Keywords: Cryptography, Algorithms, RSA, Public Key, Private Key, Information, Data, Encryption, Decryption.

KATA PENGANTAR

Segala puji penulis ucapkan kepada Allah SWT yang maha mengabulkan permohonan dan maha segalanya. Berkat petunjuk dan rahmat dari-Nya penulis dapat menyelesaikan penelitian tesis ini. Shalawat serta salam penulis persembahkan kepada "Insan Utama" Muhammad SAW sebagai manusia pemimpin umat.

Pengamanan informasi dengan menggunakan metode enkripsi merupakan cara yang biasa digunakan dalam hal pengamanan data dan informasi yang akan di kirimkan, agar data dan informasi yang dikirmkan dapat terjaga kerahasiaannya. Idenya adalah merubah data dan informasi yang dikirimkan menjadi data dan informasi yang tidak dapat dimengerti dimana untuk mengubah kebentuk yang dapat dimengerti menggunakan algoritma yang dapat mengkodekan data yang dinginkan.

Ucapan terima kasih penulis persembahkan kepada semua pihak yang telah membantu penulis dalam menyusun penelitian tesis ini:

1. Dr. Moedjiono, M.Sc, Direktur Program Pascasarjana Universitas Budi Luhur.
2. Dr. Nazori AZ, selaku Ketua Program Studi Magister Ilmu Komputer sekaligus dosen pembimbing tesis penulis yang telah bersedia membimbing dalam penyelesaian penelitian tesisini.
3. Para Dosen pengajar di Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
4. Para staff administrasi di lingkungan Pascasarjana Universitas Budi Luhur.
5. Orang tua, H. Mursyad dan Hj. Mandaini, terima kasih atas dukungan doa, semangat dan kasih sayang yang senantiasa diberikan kepada penulis.
6. Rezka Rahmalia Tanjung, S.KM, istri tercinta yang selalu memberikan semangat, dukungan, dan doa bagi penulis.
7. Ibrahim Halim, anak yang selalu jadi motivasi penulis.

8. Rekan-rekan penulis di Program Magister Ilmu Komputer Universitas Budi Luhur.

Semoga penelitian tesis ini dapat berguna untuk siapa saja yang membacanya, khususnya yang ingin mempelajari masalah keamanan data dan bahasa pemrograman *Java* khususnya *Java Server Pages (JSP).*

Penulis

Fuad Lutfi

DAFTAR ISI

halaman

DAFTAR GAMBAR

Gambar **halaman**

DAFTAR TABEL

Tabel **halaman**

LAMPIRAN

Lampiran **halaman**

DAFTAR PUSTAKA

[Amanda 2012] Amanda, Nurul., Simamora., Iskandar, Mohamad Idham. *"Implementasi Algoritma RSA untuk Perlindungan Data pada Server FT"* Naskah Publikasi Politeknik Telkom, 2012.

[Ariyus 2006] Ariyus, Dony. *Computer Security*. Andi, Yogyakarta: 2006.

[Burnett 2004] Burnett, Steve and Raine, Stephen. *RSA Security's Official Guide to Crytography*. Mc Graw Hill Osborn, California: 2004

[Chalurkar 2011] Chalurkar, Satish N., Khochare, Nilesh , Meshram, B.B. *"Survey on Modular Attack on RSA Algorithm."* IJCEM International Journal of Computational Engineering & Management, Vol. 14, October 2011.

[Deitel 2003] Deitel, Harvey M. Dan Paul J. Deitel *Java™: How To Program*, 5th Edition Prentice Hall, New Jersey: 2003.

[Flanagan 2000] Flanagan, D. *Java Examples In A Nutshell*. Sabastopol, CA: O'Reilly and Associates, 2000.

[Firasyan 2011] Firasyan, Terry. *"Penggunaan Algoritma RSA Untuk Keamanan Transaksi Online Berbasis Aplikasi Mobile"* Naskah Publikasi Institut Teknologi 10 Nopember Surabaya, 2012.

[Hariyanto 2003] Hariyanto, Bambang. *Esensi-Esensi Bahasa Pemrograman Java*. Informatika, Bandung: 2003.

[Jamgekar 2013] Jamgekar, Rajan.S., Joshi, Geeta Shantanu. *"File Encryption and Decryption Using Secure RSA"* International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.

[Kadir 2004] Kadir, Abdul. *Dasar Pemrograman Web Dinamis dengan JSP (Java Server Pages)*. Andi, Yogyakarta: 2004.

[Kadir 2005] _____. *Dasar Pemrograman Java™ 2*. Andi, Yogyakarta: 2005.

[Kurniawan 2002] Kurniawan, Budi. *Java for The Web with Servlets, JSP, and EJB: A Developers Guide to J2EE Solutions*, SAMS, 2002.

[Kurniawan 2004] Kurniawan, Yusuf. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Informatika, Bandung: 2004.