PENGAMANAN EMAIL MENGGUNAKAN ALGORITMA RSA DAN *DIGITAL SIGNATURE* SHA-1 BERBASIS *MOBILE*

TESIS

Oleh:

NURI WIYONO
1311600439

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

JAKARTA
2015

PENGAMANAN EMAIL MENGGUNAKAN ALGORITMA RSA DAN *DIGITAL SIGNATURE* SHA-1 BERBASIS *MOBILE*

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)

Oleh:

NURI WIYONO
1311600439

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 di bawah ini,

Nama Mahasiswa : Nuri Wiyono
NIM : 13116004139
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas/Program : Pascasarjana

menyatakan bahwa TESIS yang berjudul :

Pengamanan Email Menggunakan Algoritma RSA dan Digital Signature SHA-1 Berbasis Mobile

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 apabila di kemudian pernyataan ini tidak benar.

Jakarta, 24 Agustus 2015

(Nuri Wiyono)

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa	:	NURI WIYONO
Nomor Induk Mahasiswa	:	1311600439
Konsentrasi	:	REKAYASA KOMPUTASI TERAPAN
Jenjang Studi	:	STRATA 2
Judul	:	PENGAMANAN EMAIL MENGGUNAKAN ALGORITMA RSA DAN *DIGITAL SIGNATURE* SHA-1 BERBASIS *MOBILE*

Jakarta, 15 Agustus 2015

Tim Penguji : Tanda Tangan :

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

Anggota,
Dr. Ir. Nazori AZ, MT .....

Pembimbing Utama,
Mardi Hardjianto, M. Kom .....

Ketua Program Studi

(Dr. Ir. Nazori AZ, MT)

ABSTRAK

Saat ini, pengiriman data sudah banyak menggunakan media internet salah satunya adalah dengan menggunakan email. Dengan menggunakan email memungkinkan pengiriman data jarak jauh yang relative cepat dan murah. Di lain pihak pengiriman data melalui media internet sangat memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan. Pengiriman informasi melalui email menyimpan potensi berbahaya, penyalahgunaannya dapat merugikan pengirim maupun penerima pesan. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dari suatu sistem informasi. Untuk mengatasi masalah ini perlu dibuatkan sistem untuk mengamankan dan menjaga keaslian isi email, yaitu dengan menggunakan teknik enkripsi. Pada penelitian ini digunakan metode enkripsi asimetris RSA serta tanda tangan digital SHA-1 dalam pengamanan isi pesan email. Dengan algoritma kriptografi ini dapat memberikan solusi pada masalah keamanan data, yaitu masalah kerahasiaan, integritas, otentikasi serta pesan dapat terjaga keasliannya oleh orang-orang yang tidak bertangguang jawab. Berdasarkan pengujian menggunakan blackbox testing bahwa fungsionalitas sudah berjalan sesuai yang diharapkan, sedangkan hasil pengujian dengan mengadaptasi ISO 9126 didapat hasil skor sebesar 81,3% dan memiliki kriteria baik, ini berarti aplikasi yang dibuat sebagian besar sudah memenuhi kebutuhan.

Kata kunci: kriptografi, email, RSA, SHA-1, keamanan, enkripsi.

ABSTRACT

Currently, data transmission already using internet media for example using an email.Email allow sending data over long distance is relatively fast and inexpensive.. On the other hand the data transmission via the Internet it's possible the other party can be tapped into and alter transmitted data. Information transmission via email the are potential dangerous, its misuse can be detrimental to the sender or recipient of the message. Issue of security and confidentiality of data is one very important aspect of an information system. To resolve this issue should made a system to secure and maintain the authenticity of the contents of the email, by encryption techniques. This research used the RSA asymmetric encryption methods and digital signature SHA-1 in securing the contents of the email message. This cryptographic algorithm is expected to provide a solution to the problem of data security, i.e. the problem of confidentiality, integrity, authentication and message authenticity can be maintained by people who do not responsible. Testing by blackbox testing that functionality have run as expected , while the testing in adapting iso 9126 obtained the score at 81,3 % and has good criteria , this means application has met needs.

Keywords: cryptography, email, RSA, SHA-1, security, encryption.

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur kepada Allah SWT atas segala rahmat, taufik dan hidayah-Nya sehingga penulis dapat menyelesaikan penyusunan tesis dengan Judul "Pengamanan Email Menggunakan Algoritma RSA dan *Digital Signature* SHA-1 Berbasis *Mobile*". Tesis ini disusun untuk menjadi salah satu persyaratan guna menyelesaikan jenjang Strata Dua (S-2) pada Program Studi Magister Ilmu Komputer (M.Kom) Program Pascasarjana Universitas Budi Luhur Jakarta.

Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah memberikan bantuan, bimbingan dan arahan untuk penyelesaian penulisan tesis ini, dengan segala ketulusan hati penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Allah SWT atas segala Pentunjuk dan Kemudahan-Nya sehingga pada akhirnya penulis dapat menyelesaikan tesis ini.
2. Kedua orang tua serta keluarga tercinta yang tak henti-hentinya memberikan dukungan, doa dan kasih sayang.
3. Bapak Prof. Dr. Moedjiono, M.Sc. sebagai Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak. Dr. Ir. Nazori, AZ, MT. sebagai Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
5. Bapak Mardi Hardjianto, M. Kom. sebagai Dosen Program Pascasarjana Universitas Budi Luhur sekaligus sebagai pembimbing yang telah banyak memberikan saran dan masukan dalam penyusunan tesis ini.
6. Segenap Staff Pengajar dan Sekretariat tata usaha Magister Ilmu Komputer Universitas Budi Luhur yang telah memberikan ilmunya dan bantuan akademik selama penulis mengukuti pendidikan M.Kom Universitas Budi Luhur.
7. Seluruh rekan-rekan MKOM Universitas Budi Luhur, yang selalu senatiasa membantu penulis dalam setiap kegiatan perkuliahan sampai pada penulis menyusun tesis ini.

8. Semua pihak yang telah membantu penyusunan tesis ini, atas perhatian dan bantuan yang telah diberikan hingga tersusunnya tesis ini.

Penulis menyadari bahwa dalam penyusunan tesis ini masih jauh dari sempurna, terdapat kesalahan yang perlu diperbaiki dan kekurangan yang perlu dilengkapi. Demi tercapainya penulisan yang lebih baik, penulis mengharapkan kritik dan saran untuk memperbaiki dan melengkapi kekurangan tersebut.

Jakarta, Agustus 2015

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

Tabel **Halaman**

DAFTAR LAMPIRAN

Lampiran **Halaman**

DAFTAR PUSTAKA

[Acharya 2015] Acharya, Kritika, Manisha Sajwan, Sanjay Bhargava, *Analysis of Cryptographic Algorithms for Network Security.* International Journal of Computer Applications Technology and Research Volume 3– Issue 2, 130 - 135, 2014.

[Ebrahim 2013] Ebrahim , Mansoor , Shujaat Khan,Umer Bin Khalid .*Symmetric Algorithm Survey: A Comparative Analysis*. International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.

[Stiawan 2005]Stiawan, Deris. *Sistem keamanan komputer*. Elex Media Komputindo, 2005.

[Jamilia 2013] Jamilia, Aeni ,Moedjiono ,Hadi Syahrial. *Rancangan Implementasi Protokol S/MIME pada Layanan E-Mail Sebagai Upaya Peningkatan Keamanan dalam Transaksi Informasi Secara Online: Studi Kasus PT. XYZ*. Journal Technology of Information and Communication (TICOM). Vol 1, No 2, 2013.

[Haboush 2014] Haboush, Ahmad, et al. *Investigating Software Maintainability Development: A case for ISO 9126.* International Journal of Computer Science Issues, Vol. 11, Issue 2, No 2, March 2014.

[Hartono 2004] Hartono, Budi. *Ruang Lingkup Kriptografi Untuk Mengamankan Data*. Dinamika Informatika ISSN: 0854-9524, Vol.IX No.2,pp 1-7, 2004.

[Lasmana 2013] Lasmana, Indra, *Model Implementasi Keamanan Web Service dengan kriptografi dan Tanda Tangan Digital pada Sistem Informasi Akademik.* Universitas Budi Luhur, Jakarta, 2013.

[Lubis 2013] Lubis,Muhammad Safri, Muhammad Andri Budiman dan Karina Lolo Manik. *Penggunaan Algoritma RSA dengan Metode The Sieve of*