

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

TESIS



Oleh:

NURI WIYONO
1311600439

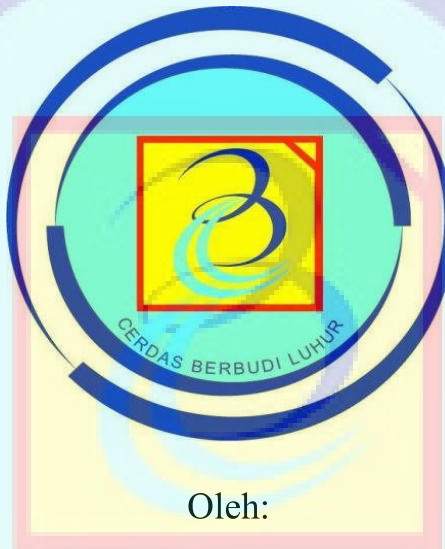
PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

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 : 1311600439
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 ijin 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 :

Ketua,
Prof. Dr. Moedjiono, M.Sc

Anggota,
Dr. Ir. Nazori AZ, MT

Pembimbing Utama,
Mardi Hardjianto, M. Kom

Tanda Tangan :

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 bertanggung 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 mengikuti pendidikan M.Kom Universitas Budi Luhur.
7. Seluruh rekan-rekan MKOM Universitas Budi Luhur, yang selalu senantiasanya 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



CERDAS BERBUDI LUHUR

DAFTAR ISI

	Halaman
ABSTRAK.....	i
<i>ABSTRACT</i>	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR	vii
DAFTAR TABEL.....	viii
DAFTAR LAMPIRAN.....	ix
BAB I PENDAHULUAN.....	1
1.1 Latar belakang.....	1
1.2 Masalah Penelitian	3
1.2.1 Identifikasi 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 PEMIKIRAN.....	8
2.1 Tinjauan Pustaka	8
2.1.1 Email	8
2.1.2 Kriptografi	10
2.1.3 Algoritma RSA.....	15
2.1.4 Fungsi Hash Satu arah	18
2.1.5 Tanda Tangan Digital	19
2.1.6 Java.....	22
2.1.7 Android.....	22

2.1.8	Kualitas Perangkat Lunak	22
2.1.9	Pengujian Sistem	23
2.1.10	ISO 9126.....	24
2.2	Tinjauan Studi	29
2.3	Tinjauan Objek Penelitian.....	37
2.4	Pola Pikir.....	37
2.5	Hipotesis.....	38
BAB III METODOLOGI PENELITIAN.....		39
3.1	Metode Penelitian.....	39
3.2	Pemilihan Sampel	40
3.3	Metode Pengumpulan Data	41
3.4	Instrumentasi	41
3.5	Teknik Analisis, Perancangan dan Pengujian Sistem	42
3.6	Langkah-Langkah Penelitian	45
3.7	Jadwal Penelitian.....	46
BAB IV PEMBAHASAN HASIL PENELITIAN.....		48
4.1	Analisa.....	48
4.2	Rancangan Sistem/Prototipe Model	50
4.3	Pengujian Sistem.....	58
4.4	Implikasi Penelitian.....	69
4.4.1	Aspek Sistem.....	69
4.4.2	Aspek Penelitian Lanjutan.....	69
4.5	Rencana Implementasi	70
BAB V PENUTUP.....		72
5.1	Kesimpulan.....	72
5.2	Saran.....	72
DAFTAR PUSTAKA.....		73
LAMPIRAN-LAMPIRAN.....		76
RIWAYAT HIDUP SINGKAT.....		90

DAFTAR GAMBAR

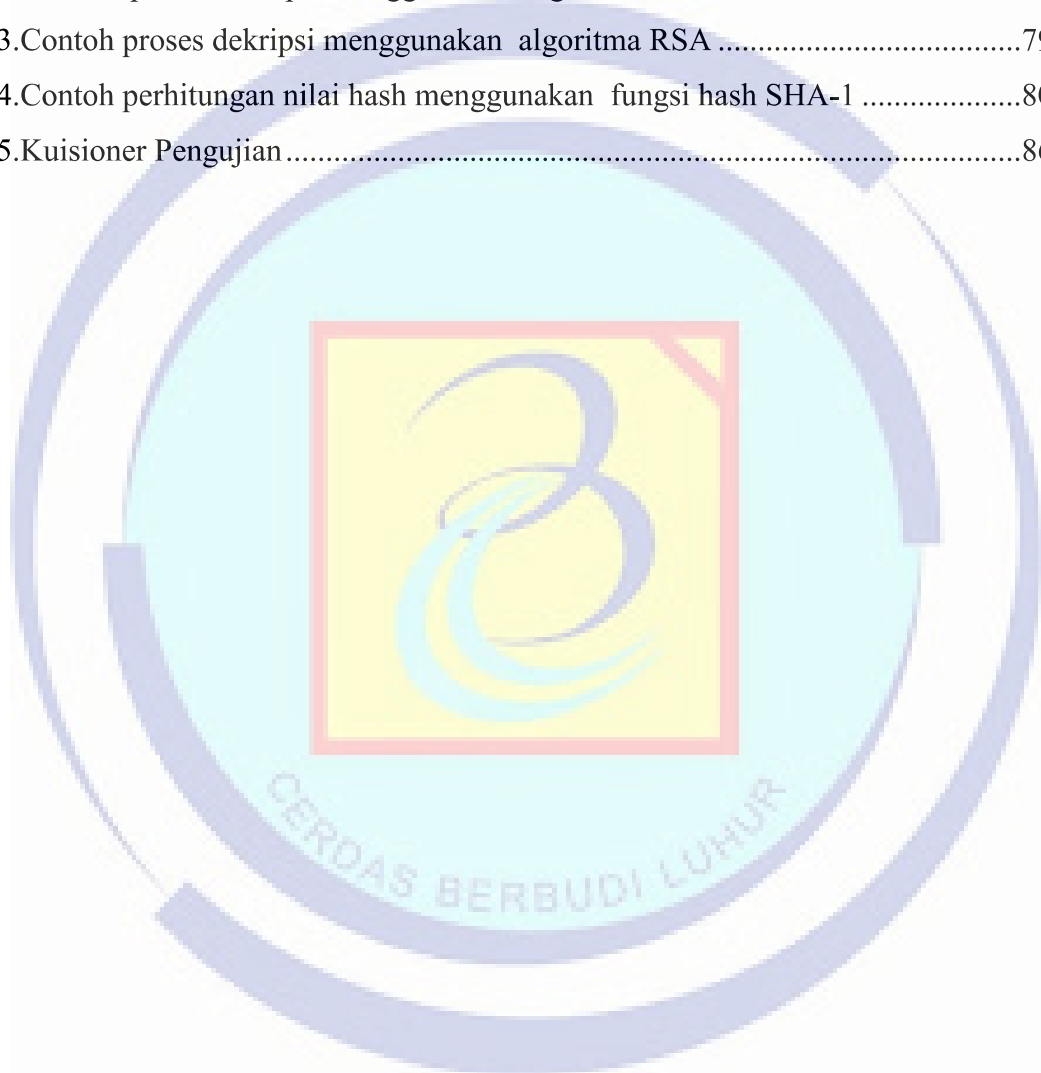
Gambar	Halaman
II-1. Klasifikasi kriptografi berdasarkan kunci yang digunakan	10
II-2. Diagram proses enkripsi dan dekripsi algoritma simetris.....	12
II-3. Diagram proses enkripsi dan dekripsi algoritma asimetris.....	13
II-4. Flowchart Enkripsi RSA	16
II-5. Flowchart Dekripsi RSA	17
II-6. Ilustrasi tanda tangan digital	20
II-7. Pola Pikir.....	37
III-1. Metode Penelitian	39
III-2. Alur proses pengiriman email.....	44
IV-1. <i>Use Case Diagram</i>	49
IV-2. Tampilan Utama	50
IV-3. Tampilan <i>Setting konfigurasi account email</i>	51
IV-4. Tampilan <i>Setting input username</i>	52
IV-5. Tampilan <i>Setting input password email</i>	52
IV-6. Tampilan <i>Setting input SMTP server email</i>	53
IV-7. Tampilan <i>Setting input port</i>	53
IV-8. Tampilan <i>Generate key</i>	54
IV-9. Tampilan <i>Compose Mail</i>	55
IV-10. Tampilan <i>Friends Key</i>	55
IV-11. Tampilan <i>Add Public Key</i>	56
IV-12. Tampilan <i>Inbox</i>	57
IV-13. Tampilan <i>Read Mail</i>	57

DAFTAR TABEL

Tabel	Halaman
II-1. Karakteristik Kualitas Model ISO 9126.....	26
II-2. Skor Penilaian	29
II-3. Tinjauan Studi	32
III-1. Jadwal Penelitian	46
IV-1. Deskripsi <i>Use Case</i>	49
IV-2. Hasil pengujian menu utama	58
IV-3. Hasil pengujian setting konfigurasi	60
IV-4. Hasil pengujian generate key.....	60
IV-5. Hasil pengujian <i>Add public key</i>	61
IV-6. Hasil pengujian <i>Compose Mail</i>	61
IV-7. Hasil pengujian <i>Inbox</i>	62
IV-8. Hasil pengujian <i>Read Mail</i>	63
IV-9. Kriteria jawaban	64
IV-10. Range Rating	65
IV-11. Aspek <i>Functionality</i>	65
IV-12. Aspek <i>Reliability</i>	66
IV-13. Aspek <i>Usability</i>	67
IV-14. Aspek <i>Efficiency</i>	67
IV-15. Pengujian Tingkat kualitas perangkat lunak keseluruhan	68
IV-16. Rencana Implementasi.....	70

DAFTAR LAMPIRAN

Lampiran	Halaman
1. Contoh pembangkitan kunci algoritma RSA	77
2. Contoh proses enkripsi menggunakan algoritma RSA	78
3. Contoh proses dekripsi menggunakan algoritma RSA	79
4. Contoh perhitungan nilai hash menggunakan fungsi hash SHA-1	80
5. Kuisisioner Pengujian	86



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*