

**PENGAMANAN PESAN YAHOO MESSENGER DENGAN
HYBRID CRYPTOSYSTEM KOMBINASI RSA DAN
VIGENERE DOUBLE COLUMNAR TRANSPOSITION
BERBASIS ANDROID**

TESIS



Oleh:

Ahmad Pudoli

1211601420

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

**PENGAMANAN PESAN YAHOO MESSENGER DENGAN
HYBRID CRYPTOSYSTEM KOMBINASI RSA DAN
VIGENERE DOUBLE COLUMNAR TRANSPOSITION
BERBASIS ANDROID**

TESIS

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



Oleh:

Ahmad Pudoli

1211601420

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015



**PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Ahmad Pudoli
NIM : 1211601420
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputasi Terapan
Program/Fakultas : Pasca Sarjana

Menyatakan bahwa Tesis yang berjudul:

**PENGAMANAN PESAN YAHOO MESSENGER DENGAN HYBRID
CRYPTOSYSTEM KOMBINASI RSA DAN VIGENERE DOUBLE
COLUMNAR TRANSPOSITION BERBASIS ANDROID**

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik 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, 20 Februari 2015



(Ahmad Pudoli)



PROGRAM STUDI: MAGISTER ILMU KOMPUTER

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama : Ahmad Pudoli
NIM : 1211601420
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul : Pengamanan Pesan Yahoo Messenger dengan Hybrid Cryptosystem Kombinasi RSA dan Vigenere Double Columnar Transposition Berbasis Android

Jakarta, 7 Maret 2015

Tim Penguji :

Tanda tangan :

Ketua,
Prof. Dr. Moedjiono, M.Sc

Anggota / Pembimbing Utama,
Dr. Ir. Nazori Az, M.T

Pembimbing Pendamping,
Mardi Hardjianto, M.Kom

Ketua Program Studi

Dr. Ir. Nazori Az, M.T

ABSTRAK

Perkembangan Teknologi Informasi membuat seseorang dengan mudah mendapatkan informasi, dan komunikasi juga dapat dilakukan dimanapun dan kapanpun. *Yahoo Messenger* merupakan layanan yang dapat digunakan untuk melakukan komunikasi melalui jaringan internet. Namun, tidak ada pengamanan pada pesan yang dikirim oleh layanan tersebut. Jika ada seseorang melakukan serangan contohnya *sniffing*, maka dapat dengan mudah pesan dapat dibaca. Hal ini dapat merugikan pengguna, terlebih pesan tersebut bersifat rahasia. Untuk mengantisipasi agar pesan tidak mudah dibaca oleh orang yang tidak berhak, maka perlu dibuat sistem pengamanan pada pesan tersebut. Salah satu cara untuk melakukan pengamanan tersebut adalah dengan enkripsi. Banyak teknik kriptografi yang dapat digunakan. Pada penelitian ini, digunakan *Hybrid Cryptosystem* dengan kombinasi RSA dan *Vigenere* modifikasi *Double Columnar Transposition*. Untuk menjaga keabsahan dari pesan yang dikirim perlu ditambahkan teknik *error detection* yang dalam hal ini menggunakan *hash function*. Pada penelitian ini menghasilkan aplikasi yang dapat meningkatkan keamanan pesan *Yahoo Messenger*, dimana pesan tersebut dienkripsi dengan metode *Hybrid Cryptosystem* kombinasi RSA dan *Vigenere Double Columnar Transposition*.

Kata kunci : Kriptografi, *Hybrid Cryptosystem*, *RSA*, *Vigenere*, *Double Columnar Transposition*

ABSTRACT

The development of information technology makes people easily get information, and communication can also be done anywhere and anytime. Yahoo Messenger is a service that can be used to communicate through the Internet. However, there is no security in the message sent by the service. For the example If there is someone with sniffing attack, it can easily readable message. It can be harmful to the user, especially the message is confidential. To anticipate that the message is not readable by unauthorized people, it needs to make the security system on the message. One way to do that is with encryption security. Many cryptographic techniques that can be used. In this study, use Hybrid Cryptosystem with a combination of RSA and Vigenere modification Double Columnar transposition. To maintain the validity of the message sent should be added error detection techniques, in this case using a hash function. In this research, produce applications that can enhance security Yahoo Messenger messages, where the messages are encrypted with RSA combination methods Hybrid Cryptosystem and Vigenere Double Columnar transposition.

Keywords : Cryptography, Hybrid Cryptosystem, RSA, Vigenere, Double Columnar Transposition

KATA PENGANTAR

Puji dan Syukur yang sedalam-dalamnya kepada Allah SWT, karena hanya dengan rahmat dan karunia-Nya-lah naskah proposal tesis yang berjudul “Pengamanan Pesan Yahoo Messengger Dengan Hybrid Cryptosystem Kombinasi RSA dan Vigenere Double Columnar Transposition Berbasis Android” dapat diselesaikan. Shalawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang tulus kepada:

1. Bapak dan Ibu yang senantiasa memberikan kasih sayang, nasihat, dukungan semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
2. Istriku Dewi Kusumaningsih dan anak saya Defandra Fathi Al-Akhtar, yang selalu memberikan kebahagiaan dan keceriaan.
3. Bapak Prof. Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana Universitas Budi Luhur.
4. Bapak Dr. Ir. Nazori AZ, M.T. selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur dan selaku pembimbing yang banyak membimbing dan memberi masukan dalam penyusunan tesis ini..
5. Bapak Mardi Hardjianto, M.Kom, selaku pembimbing tesis yang banyak memberikan bimbingan, bantuan dan tak henti-hentinya memberikan dukungan.
6. Seluruh Dosen Program Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
7. Serta semua pihak yang tidak dapat dituliskan.

Penulis menyadari bahwa penulisan tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, Februari 2015

Ahmad Pudoli

DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR	vii
DAFTAR TABEL	viii
DAFTAR LAMPIRAN.....	ix
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	2
1.2.1 Identifikasi Masalah.....	2
1.2.2 Batasan Masalah	2
1.2.3 Rumusan Masalah.....	2
1.3 Tujuan dan Manfaat Penelitian.....	3
1.3.1 Tujuan Penelitian.....	3
1.3.2 Manfaat Penelitian.....	3
1.4 Sistematika Penulisan.....	3
1.5 Definisi dan Istilah	4
BAB II LANDASAN PEMIKIRAN	6
2.1 Tinjauan Pustaka	6
2.1.1 Kriptografi	6
2.1.2 RSA (Rivest-Shamir-Adleman).....	8
2.1.3 <i>Vigenere Cipher</i>	10
2.1.4 Modifikasi <i>Vigenere Cipher</i> dengan Kombinasi <i>Double Columnar Transposition</i>	12
2.1.5 <i>Hybrid Cryptosystem</i>	16
2.1.6 <i>Checksum</i>	17
2.1.7 Pengujian <i>Black Box</i>	17
2.1.8 Pengujian Kualitas Perangkat Lunak ISO 9126	18
2.1.9 Sistem Operasi Android.....	21
2.2 Tinjauan Studi	22
2.3 Tinjauan Objek Penelitian	35
2.1.1 Perangkat Keras	35
2.1.2 Perangkat Lunak	36

2.4	Pola Pikir	36
2.5	Hipotesis	38
BAB III DESAIN PENELITIAN.....		39
3.1	Metode Penelitian.....	39
3.2	Metode Pengumpulan Data	39
3.3	Sumber Data	39
3.4	Teknik Analisis Data	40
3.5	Langkah-langkah Penelitian	40
3.5.1	Pengumpulan Data dan Informasi	40
3.5.2	Identifikasi Kebutuhan.....	43
3.5.3	Menentukan Metode Cryptosystem.....	44
3.5.4	Desain Sistem	45
3.5.5	Pembuatan Sistem.....	55
3.5.6	Pengujian dan Analisis	55
3.5.7	Penarikan Kesimpulan.....	55
3.6	Jadwal Penelitian	56
BAB IV PEMBAHASAN HASIL PENELITIAN.....		57
4.1	Tampilan Aplikasi	57
4.1.1	Tampilan <i>Form Login</i>	57
4.1.2	Tampilan <i>Form</i> Daftar Teman.....	57
4.1.3	Tampilan <i>Form Chat</i>	58
4.2	Pengujian Perangkat Lunak.....	59
4.2.1	Lingkungan Pengujian Perangkat Lunak.....	59
4.2.2	Pengujian dengan <i>Black Box</i>	60
4.2.3	Pengujian Error Detection	63
4.2.4	<i>Sniffing Chat</i> dengan <i>Cain and Abel</i> dan <i>Wireshark</i>	66
4.2.5	Pengujiuan Kualitas Perangkat Lunak Mengadaptasi Kriteria ISO 9126	69
4.3	Implikasi Penelitian	74
4.3.1	Aspek Sistem	74
4.3.2	Aspek Manajerial.....	76
4.3.3	Aspek Penelitian Lanjutan.....	76
4.4	Rencana Implementasi.....	76

BAB V PENUTUP.....	78
5.1 Kesimpulan.....	78
5.2 Saran.....	79
5.3 Implikasi Penelitian	79
5.4 Rencana Implementasi.....	80
DAFTAR PUSTAKA	81



DAFTAR GAMBAR

Gambar	Halaman
II-1 : Skema Penggunaan Algoritma Simetris.....	7
II-2 : Skema Penggunaan Algoritma Asimetris	8
II-3 : Tabel <i>Vigenere Ciphe</i>	11
II-4 : Pola Pikir	36
III-1 : Langkah-langkah Penelitian.....	40
III-2 : Perbandingan Pola Aliran Paket Data	41
III-3 : Proses Meracuni ARP Target dengan <i>Cain And Abel</i>	42
III-4 : <i>Sniffing</i> Paket Data dengan <i>Wireshark</i>	43
III-5 : Gambaran Umum Sistem yang Dibangun.....	46
III-6 : Proses Mengambil Kunci dari Server dan Mengirim Kunci Ke Teman	46
III-7 : Desain Enkripsi dengan <i>Hybrid Cryptosystem</i> Usulan	47
III-8 : Desain Dekripsi dengan <i>Hybrid Cryptosystem</i> Usulan.....	48
III-9 : Protokol Pesan.....	49
III-10 : Enkripsi <i>Vigenere</i> dengan Kombinasi <i>Double Columnar Transposition (DCT)</i>	51
III- 11 : Dekripsi <i>Vigenere</i> dengan Kombinasi <i>Double Columnar Transposition (DCT)</i>	53
IV-1 : Tampilan <i>Form Login</i>	57
IV-2 : Tampilan <i>Form</i> Daftar Teman	58
IV-3 : Tampilan <i>Form Chat</i>	58
IV-4 : Proses Pengiriman Pesan Pada Pengujian <i>Error Detection</i>	64
IV-5 : Perubahan Pesan Pada Pengujian <i>Error Detection</i>	65
IV-6 : Proses Pengiriman Pesan yang Sudah Diubah Pada Pengujian <i>Error Detection</i>	65
IV-7 : Meracuni ARP Target Pengujian	67
IV-8 : Pesan Dikirim Dari Aplikasi <i>Yahoo Messenger</i>	68
IV-9 : Pesan yang Dikirim Melalui Aplikasi Yang Dibangun.....	68
IV-10 : Arsitektur Sistem Yang Dibangun	75

DAFTAR TABEL

Tabel		Halaman
II-1	: Karakteristik Kualitas <i>Software</i> Sesuai ISO 9126.....	19
II-2	: Skor Penilaian	20
II-3	: <i>Rating Scale</i>	21
II-4	: Ringkasan Penelitian Terdahulu.....	30
III-1	: Tipe Pesan yang Digunakan Pada Sistem	49
III-2	: Skala Pengukuran	55
III-3	: Jadwal Penelitian.....	56
IV-1	: Hasil Pengujian <i>Form Login</i> dengan menggunakan <i>Black Box</i>	60
IV-2	: Hasil Pengujian <i>Form</i> Daftar Teman dengan menggunakan <i>Black Box</i>	61
IV-3	: Hasil Pengujian <i>Form Chat</i> dengan menggunakan <i>Black Box</i>	62
IV-4	: Kriteria Presentase Tanggapan Responden Terhadap Skor Ideal	70
IV-5	: Skor Aspek <i>Functionality</i>	70
IV-6	: Skor Aspek <i>Reliability</i>	71
IV-7	: Skor Aspek <i>Usability</i>	72
IV-8	: Skor Aspek <i>Efficiency</i>	72
IV-9	: <i>Rating Akhir</i>	73
IV-10	: Rencana Implementasi	77

DAFTAR LAMPIRAN

Lampiran		Halaman
1	Hasil Pengujian Fungsional dengan Black Box.....	83
2	Kuesioner Pengujian Kualitas dengan Mengadaptasi ISO 9126	86



DAFTAR PUSTAKA

- [Abutaha 2011] Abutaha, Mohammed, et.al. "Cryptography is The Science of Information Security", *Communication Theory of Secrecy Systems*, Vol.5, No.3, Juli 2011.
- [Anjagou 2013] Patil, Anjali and Rajeshwari Goudaar. "A Comparative Survey Of Symetric Encryption Techniques For Wireless Devices". *International Journal Of Scientific and Technology Research (IJSTR)*, Vol. 2, No. 8, Agustus 2013.
- [Anjana 2014] Chandran, Anjana S. "Repeated Encryption on RSA", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, Vol. 4, No. 4, April 2014.
- [Fafa 2014] Ali, Fairous Mushtaq Sher and Falah Hassan Sarhan. "Enhancing Security of Vigenere Cipher by Stream Cipher", *International Journal of Computer Application*, Vol. 100, No. 1, Agustus 2014.
- [Geomar 2013] Mateescu, Georgiana and Marius Vladescu. "A Hybrid Approach of System Security for Small and Medium Enterprises: combining different Cryptography techniques". *Federated Conference on Computer Science and Information System*, (2013):659-662.
- [Gutub 2010] Gutub, Adnan Abdul-Aziz. "Pixel Indicator Technique for RGB Image Steganography". *Journal of Emerging Technologies in Web Intelligence*, Vol.2, No.1, Februari 2010.
- [Hendrasukiman 2012] Hendra and Sukiman. "Aplikasi Pengaman Pertukaran SMS pada Perangkat Android dengan Metode RSA". *Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM)*, 2012.
- [Irena 2006] Jovanović, Irena. "Software Testing Methods and Techniques". *The IPSI BgD Transactions on Internet Research*, Vol. 30, 2006.
- [Jigar 2013] Chauhan, Jigar, et.al. "Enhancing Data Security by using Hybrid Cryptography Algorithm". *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 2, No. 3, Mei 2013.
- [Krisstef 2012] Kristoforus and Stefanus Aditya. "Implementasi Algoritma Rijndael Untuk Enkripsi dan Dekripsi Pada Citra Digital". *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, Juni 2012.
- [Mansoor 2013] Ebrahim, Mansoor, et.al. "Symetric Algorithm Survey: A Comparative Analysis". *International Journal of Applications*, Vol. 61, No. 20, Januari 2013.