

LAPORAN TUGAS AKHIR

Topik Tugas Akhir:

Kajian Murni Matematika

**PENGGUNAAN TEOREMA EULER PADA KRIPTOGRAFI RSA (RIVEST, SHAMIR
DAN ADLEMAN) DENGAN BAHASA PEMROGRAMAN MATLAB**

TUGAS AKHIR

Diajukan Kepada Fakultas dan Ilmu Pendidikan

Universitas Muhammadiyah Malang

Sebagai Salah Satu Prasyarat untuk Mendapatkan

Gelar Sarjana Pendidikan Matematika



Oleh:

INTAN PERMATASARI

NIM: 201110060311081

**PROGRAM STUDI PENDIDIKAN MATEMATIKA
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS MUHAMMADIYAH MALANG**

2015

LEMBAR PENGESAHAN

Dipertahankan di depan Dewan Penguji Tugas Akhir
Program Studi Pendidikan Matematika
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Muhammadiyah Malang
dan Diterima Untuk Memenuhi Persyaratan
Memperoleh Gelar Sarjana (S1)
Pendidikan Matematika
pada Tanggal: 09 Juli 2015



Dewan Penguji:

1. Alfiani Athma Putri, M.Pd
2. Agung Deddiliawan Ismail, M.Pd
3. Moh. Mahfud Effendi, Dr., M.M
4. Siti Inganah, Dra., M.Pd

Tanda Tangan

1. 
2. 
3. 
4. 

KATA PENGANTAR

Puji syukur Alhamdulillah kepada Allah SWT yang Maha Mengetahui lagi Maha Penyayang, karena dengan rahmat dan hidayah-Nya, penulis dapat menyelesaikan Tugas Akhir dengan judul “Penggunaan Teorema Euler pada Kriptografi RSA (Rivest, Shamir dan Adleman) dengan Bahasa Pemrograman Matlab”. Shalawat serta salam semoga tercurah kepada Rosulullah SAW, keluarga dan para sahabatnya.

Penulisan Tugas Akhir ini merupakan kajian teori yang menggunakan metode studi literature (*Library Research*) atau studi kepustakaan, yaitu pembahasan yang dilakukan dengan mengkaji teori-teori atau literatur-literatur yang relevan untuk memecahkan masalah.

Penulis menyadari bahwa tugas akhir ini dapat terselesaikan berkat bimbingan, bantuan dan motivasi dari banyak pihak. Oleh karena itu dengan ketulusan hati penulis menghanturkan rasa hormat dan terimakasih kepada:

1. Moh. Mahfud Effendi, Dr., M.M, selaku dosen pembimbing I yang telah meluangkan waktu dan kesabaran dalam memberi petunjuk, bimbingan dan pengarahan kepada penulis sehingga terselesainya tugas akhir ini.
2. Siti Inganah, Dra, M.Pd., selaku dosen pembimbing II yang telah memberikan pengarahan dan bimbingan kepada penulis sehingga terselesainya tugas akhir ini.

Semoga Allah Swt menunjukkan jalan dan memberikan Cahaya-Nya, serta melapangkan dada kita dengan limpahan iman dan keindahan tawakal kepada-Nya.

Penulis berharap semoga Tugas Akhir ini bermanfaat bagi semua pihak yang berkepentingan. Namun demikian tiada manusia yang sempurna, oleh karena itu kritik dan saran yang membangun sangat kami harapkan untuk menjadikan Tugas Akhir ini lebih sempurna.

Malang,

Penulis

DAFTAR ISI

Halaman Judul	i
Lembar Persetujuan	ii
Lembar Pengesahan	iii
Halaman Pernyataan Keaslian	iv
Halaman Motto	v
Halaman Persembahan	vi
Kata Pengantar	vii
Abstrak	viii
Abstrack	ix
DAFTAR ISI	x
Daftar Tabel	xii
Daftar Gambar	xiii
Daftar Lampiran	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Pembatasan Masalah	4
1.4 Tujuan Kajian	4
1.5 Manfaat Kajian	4
1.6 Metode Pembahasan	4
BAB II LANDASAN TEORI	6
2.1 Kerangka Konseptual	6
2.2 Pesan	7
2.3 Teks	8
2.4 Penyandian	8
2.5 Teori Matematika	9
2.6 Kriptografi	15
2.7 Kode ASCII	18
2.8 Algoritma RSA	19
2.9 Bahasa Pemrograman Matlab	22
BAB III PEMBAHASAN	31
3.1 Konversi Teks dalam Kode ASCII	31
3.2 Penyandian dalam Kriptografi RSA	32
3.2.1 Pembangkitan Kunci Kriptografi RSA	33
3.2.2 Proses Enkripsi pada Kriptografi RSA	39

3.2.3 Proses Dekripsi pada Kriptografi RSA	41
3.3 Konversi Kode ASCII dalam Teks	44
BAB IV KESIMPULAN DAN SARAN	45
4.1 Kesimpulan	45
4.2 Saran	46
Daftar Pustaka	47
Lampiran	48



DAFTAR LAMPIRAN

Lampiran A Penghitungan Manual Enkripsi	48
Lampiran B Penghitungan Manual Dekripsi	52



Daftar Pustaka

Aris, Sugiarto. 2006. *Pemrograman GUI dengan Matlab*. Yogyakarta: Andi Offset.

Ariyus, Doni. 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta: CV. Andi Offset

Buchmann, Johannes A. 2000. *Introduction to Cryptography*. New York : Springer-Verlag.

Dooley, John F. 2013. *A Brief History of Cryptology and Cryptographic Algorithm*. New York: Troubador.

Hariato. 2003. *Berbahasa Indonesia dan Makna*. Yogyakarta: ANDI.

Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Bandung: Informatika Bandung.

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan*. Yogyakarta: ANDI Yogyakarta.

Stinson, Douglas. 2002. *Cryptography Theory and Practice*. Kansas: e-book.

Taufik, Marhan. 1999. *Pengantar Teori Bilangan*. Malang: Universitas Muhammadiyah Malang

Vaudenay, Serge. 2005. *A Classical Introduction to Cryptography*. New York: Springer.

Widiarsono, Teguh. 2005. *Tutorial Praktis Belajar Matlab*. Jakarta : e-book