**ENKRIPSI FILE TEKS MENGGUNAKAN ALGORITMA**

**RIVEST-SHAMIR-ADLEMAN (RSA)**

TUGAS AKHIR



Oleh:

**ELVAND ANDRIAN MANURUNG**

NIM. 14615073

KEMENTERIAN RISET TEKNOLOGI DAN PENDIDIKAN TINGGI

POLITEKNIK NEGERI SAMARINDA

JURUSAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK INFORMATIKA

SAMARINDA 2017

**ENKRIPSI FILE TEKS MENGGUNAKAN ALGORITMA**

**RIVEST-SHAMIR-ADLEMAN (RSA)**

Diajukan sebagai persyaratan untuk memenuhi derajat Ahli Madya (Amd) pada  
Program Studi Teknik Informatika  
Jurusan Teknik Informasi  
Politeknik Negeri Samarinda

TUGAS AKHIR



Oleh:

**ELVAND ANDRIAN MANURUNG**

NIM. 14615073

KEMENTERIAN RISET TEKNOLOGI DAN PENDIDIKAN TINGGI

POLITEKNIK NEGERI SAMARINDA

JURUSAN TEKNOLOGI INFORMASI

PROGRAM STUDI TEKNIK INFORMATIKA

**HALAMAN PERNYATAAN ORISINALITAS**

Saya yang bertanda tangan di bawah ini :

Nama : Elvand Andrian Manurung

NIM : 14615073

Jurusan : Teknologi Informasi

Program Studi : Teknik Informatika

Jenjang : Diploma III

Judul Tugas Akhir : Enkripsi File Teks Menggunakan Algoritma Rivest-Shamir-Adleman (RSA)

Dengan ini menyatakan bahwa Laporan Tugas Akhir ini adalah hasil karya saya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Jika dikemudian hari terbukti ditemukan unsur plagirisme dalam Laporan Tugas Akhir ini, maka saya tersedia menerima sanksi sesuai peraturan perundangan-undangan yang berlaku.

Samarinda, 05 Agustus 2017

Elvand Andrian Manurung  
 NIM. 14615073

# HALAMAN PENGESAHAN PEMBIMBING

**ENKRIPSI FILE TEKS MENGGUNAKAN ALGORITMA**

**RIVEST-SHAMIR-ADLEMAN (RSA)**

**NAMA : ELVAND ANDRIAN MANURUNG**

**NIM : 14615073**

**JURUSAN : TEKNOLOGI INFORMASI**

**PROGRAM STUDI : TEKNIK INFORMATIKA**

**JENJANG STUDI : DIPLOMA III**

**Laporan Tugas Akhir ini telah disahkan**

**pada tanggal, 30 Agustus 2017 2015**

**Menyetujui :**

**Pembimbing I, Pembimbing II,**

**Rihartanto, ST. Agusma Wajiansyah, S.ST., MT.**

**NIP. 19711205 200312 1 001 NIP.** **19810805 200501 1 003**

**Mengesahkan :**

**Direktur Politeknik Negeri Samarinda,**

**Ir. H. Ibayasid, M.Sc.**

**NIP.19590303 198903 1 002**

**Lulus Ujian Tanggal : 05 Agustus 2017**

# HALAMAN PERSETUJUAN PENGUJI

**ENKRIPSI FILE TEKS MENGGUNAKAN ALGORITMA**

**RIVEST-SHAMIR-ADLEMAN (RSA)**

**NAMA : ELVAND ANDRIAN MANURUNG**

**NIM : 14615073**

**JURUSAN : TEKNOLOGI INFORMASI**

**PROGRAM STUDI : TEKNIK INFORMATIKA**

**JENJANG STUDI : DIPLOMA III**

**Laporan Tugas Akhir ini telah diuji dan disetujui**

**pada tanggal, 24 Agustus 2017**

**Dewan Penguji :**

**Penguji I,**

**Nama : Arief Bramanto Wicaksono Putra, S.ST., MT**

**NIP : 19830120 200801 1 006** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Penguji II,**

**Nama : Supriadi, S.ST., MT**

**NIP : 19760427 200501 1 001** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Penguji III,**

**Nama : Wahyuni Eka Sari, S.Kom., M.Eng**

**NUP :** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Mengetahui :**

**Ketua Jurusan Ketua Program Studi**

**Teknologi Informasi, Teknik Informatika,**

**Ansar Rizal, ST., M.Kom Farindika Metandi, BCompSc., MM., M.Cs**

**NIP. 19700809 199903 1 001 NIP. 19870308 200801 1 002**

# ABSTRAK

Kerahasiaan merupakan salah satu aspek penting dari informasi. Saat ini, keamanan terhadap informasi data yang tersimpan dalam *file* sudah menjadi persyaratan mutlak. *Kriptografi* merupakan solusi dalam hal menjaga kemanan dan kerahasian informasi dalam bentuk data pada *file.* Pada penelitian ini diterapkan algoritma *Rivest-Shamir-Adleman* (RSA) pada proses enkripsi *file* teks untuk melindungi data agar tetap aman. Algoritma RSA menggunakan kunci asimteris. Kunci asimetris dibangun berdasarkan pasangan bilangan prima. Implementasi algoritma RSA untuk proses enkripsi dan dekripsi berhasil dilakukan. Dalam penelitian ini pasangan bilangan prima terkecil yang berhasil diimplementasikan dalam penelitian ini adalah 11 dan 13, dan bilangan prima terbesar dibatasi maksimal 997.

**Kata Kunci :** Kriptografi, RSA, Kunci Asimetris

# *ABSTRACT*

*Confidentiality is an important aspect of information. Currently, security of an information stored in a file is required. Cryptography is a solution in terms of maintaining security and confidentiality of an information. In this research Rivest-Shamir-Adleman (RSA) algorithm is applied in text file encryption to protect data and to keep it safe. RSA algorithm uses asymteric keys. Asymmetric keys are built on the prime pair. In this research, implementation of RSA algorithm for encryption and decryption process successfully done. The pair of the smallest primes that have been successfully implemented in this study are 11 and 13, and the biggest prime is 997.*

***Keyword :*** *Cryptography, RSA, Asymmetric Key*

# KATA PENGANTAR

Puji syukur dan terima kasih kepada Tuhan Yang Maha Esa. Dan kepada kedua orang tua penulis yang selalu mendoakan serta memberikan dukungan moral dan material kepada penulis dalam mengerjakan laporan tugas akhir sehingga penulis dapat menyelesaikan Laporan tugas akhir yang berjudul “Enkripsi File Teks Menggunakan Algoritma Rivest-Shamir-Adleman (RSA)”. Terselesaikannya Laporan Tugas Akhir ini hanyalah setapak kecil permulaan dari perjalanan panjang yang masih harus ditempuh.

Laporan Tugas Akhir ini adalah salah satu persyaratan akhir Program D3 Konsentrasi Teknik Informatika Jurusan Teknologi Informasi Politeknik Negeri Samarinda.

Ucapan terima kasih disampaikan kepada semua pihak yang secara langsung maupun tidak langsung memberikan dukungan dan bantuannya hingga terselesaikannya Laporan Tugas Akhir ini. Ucapan terima kasih khusus di sampaikan kepada :

1. Bapak Ir. H. Ibayasid, M.Sc. selaku Direktur Politeknik Negeri Samarinda.
2. Bapak Ansar Rizal, ST., M.Kom. selaku Ketua jurusan Teknologi Informasi Politeknik Negeri Samarinda.
3. Bapak Farindika Metandi, BCompSc., MM., M.Cs. selaku Ketua Program Studi Teknik Informatika.
4. Bapak Rihartanto, ST. selaku Pembimbing 1 dan Bapak Agusma Wajiansyah, S.ST., MT. selaku Pembimbing 2 yang telah memberikan bimbingan dan masukan kepada penulis dalam menyelesaikan laporan tugas akhir ini.
5. Bapak Arief Bramanto W.P, S.ST., M.T. selaku Koordinator Kelompok Riset Dosen.
6. Semua rekan-rekan sesama mahasiswa Jurusan Teknologi Informasi.

Saran yang bersifat membangun sangat diharapkan untuk kesempurnaan Laporan Tugas Akhir ini. Semoga Laporan Tugas Akhir ini menjadi sumber inspirasi positif dan untuk dapat lebih bermanfaat bagi para pembaca baik yang dalam tahap pembelajaran ataupun untuk menambah luasnya pengetahuan.

Samarinda, 05 Agustus 2017

Penulis

# DAFTAR ISI

[ABSTRAK v](#_Toc491704677)

[ABSTRACT vi](#_Toc491704678)

[KATA PENGANTAR vii](#_Toc491704679)

[DAFTAR ISI ix](#_Toc491704680)

[DAFTAR GAMBAR xi](#_Toc491704681)

[DAFTAR TABEL xii](#_Toc491704682)

[BAB I PENDAHULUAN 1](#_Toc491704683)

[1.1 Latar Belakang 1](#_Toc491704684)

[1.2 Rumusan Masalah 2](#_Toc491704685)

[1.3 Batasan Masalah 2](#_Toc491704686)

[1.4 Tujuan Penelitian 2](#_Toc491704687)

[1.5 Manfaat Penelitian 3](#_Toc491704688)

[BAB II TINJAUAN PUSTAKA 4](#_Toc491704689)

[2.1 Kajian Ilmiah 4](#_Toc491704690)

[2.2 Dasar Teori 5](#_Toc491704691)

[2.2.1 Mekanisme Kriptografi 9](#_Toc491704692)

[2.2.2 Macam Macam Algoritma Kriptografi Modern 10](#_Toc491704693)

[2.2.3 Algoritma Cipher Pada Proses Asimetris Dan Simetris 11](#_Toc491704694)

[2.2.4 Algoritma Rivest-Shamir-Adleman (RSA) 12](#_Toc491704695)

[BAB III KERANGKA KONSEP DAN METODOLOGI PENELIT 17](#_Toc491704696)

[3.1 Kerangka Konsep Penelitian 17](#_Toc491704697)

[3.1.1 Kriptografi 17](#_Toc491704698)

[3.1.2 Algoritma Rivest-Shamir-Adleman (RSA) 18](#_Toc491704703)

[3.1.3 File Teks 19](#_Toc491704704)

[3.2 Metode Penelitian 20](#_Toc491704705)

[3.2.1 Riset Awal 21](#_Toc491704706)

[3.2.2 Perancangan 21](#_Toc491704707)

[3.2.3 Pengujian 22](#_Toc491704708)

[3.2.4 Analisa Hasil 22](#_Toc491704709)

[3.3 Variabel Penelitian 22](#_Toc491704710)

[3.4 Data dan Tempat Penelitian 23](#_Toc491704711)

[BAB IV HASIL DAN PEMBAHASAN 24](#_Toc491704712)

[4.1 Proses Enkripsi Dan Dekripsi File Teks 24](#_Toc491704713)

[4.1.1 Menghitung Kunci Publik 24](#_Toc491704714)

[4.1.2 Menghitung Kunci Privat 26](#_Toc491704715)

[4.2 Proses Enkripsi menggunakan Kunci Publik 28](#_Toc491704716)

[4.3 Proses Dekripsi Menggunakan Kunci Privat 33](#_Toc491704717)

[4.5 Pengujian 38](#_Toc491704718)

[4.6 Analisa Hasil 43](#_Toc491704719)

[BAB V PENUTUP 44](#_Toc491704720)

[5.1 Kesimpulan 44](#_Toc491704721)

[5.2 Saran 44](#_Toc491704722)

**DAFTAR PUSTAKA 45**

# DAFTAR GAMBAR

[Gambar 2.2 Mekanisme Kriptografi](#_Toc487146642) 9

[Gambar 2.3 Proses Algoritma Simetri](#_Toc487146643) 10

[Gambar 2.4 Proses Algoritma Asimetris](#_Toc487146644) 11

Gambar 2.5 Tabel ASCII ............................................................................................... 13

[Gambar 3.1 Diagram Alir Kerangka Konsep Penelitian](#_Toc487146645) 17

[Gambar 3.2 Diagram Alir Metodologi Penelitian](#_Toc487146646) 20

[Gambar 4.1 Flowchart Proses Menghitung Kunci Publik RSA](#_Toc487146647) 25

[Gambar 4.2 Flowchart Proses Menghitung Kunci Privat RSA](#_Toc487146648) 27

[Gambar 4.3 Flowchart Enkripsi Pesan Dengan Menggunakan Algoritam RSA](#_Toc487146649) 29

[Gambar 4.4 Flowchart Proses Enkripsi Menggunakan Kunci Publik](#_Toc487146650) 30

Gambar 4.5 Flowchart Dekripsi Pesan Dengan Menggunakan Algoritam RSA …...... 34

Gambar 4.6 Flowchart Proses Dekripsi Menggunakan Kunci Privat …....................... 35

# DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu 5

Tabel 2.2 Hasil Enkripsi 14

Tabel 2.3 Enkripsi Code 15

Tabel 2.4 Deskripsi Code 16

Tabel 4.1 Prose Enkripsi Menggunakan Kunci Publik 31

Tabel 4.2 Proses Deskripsi Menggunakan Kunci Privat 36

Tabel 4.3 Plain Char Dan ASCII Number 38

Tabel 4.4 Hasil Enkripsi Pada Program 39

Tabel 4.5 Hasil Dekripsi Pada Program 39

Tabel 4.6 Plain Char Dan ASCII Number 40

Tabel 4.7 Hasil Enkripsi Pada Program 41

Tabel 4.8 Hasil Dekripsi Pada Program 42