

TUGAS AKHIR
PENGAMANAN DOKUMEN MENGGUNAKAN
KOMBINASI METODE *RSA (RIVEST SHAMIR*
ADLEMAN) DAN VIGENERE CIPHER



Disusun Untuk Memenuhi Syarat Menyelesaikan Tugas Akhir Pendidikan
Sarjana Terapan Telekomunikasi Pada Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi
Politeknik Negeri Sriwijaya

Oleh :

Nama : Ardelia Nidya Agustina (0613 4035 1618)

Dosen Pembimbing I : Aryanti, S.T., M.Kom

Dosen Pembimbing II : Nasron, S.T., M.T

POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2017

**PENGAMANAN DOKUMEN MENGGUNAKAN KOMBINASI
METODE RSA (RIVEST SHAMIR ADLEMAN) DAN
VIGENERE CIPHER**



TUGAS AKHIR

**Disusun Untuk Memenuhi Syarat Menyelesaikan Pendidikan
Sarjana Terapan Pada Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi
Politeknik Negeri Sriwijaya**

Oleh:

**ARDELIA NIDYA AGUSTINA
0613 4035 1618**

Menyetujui,

Pembimbing I

**Aryanti, S.T., M.Kom.
NIP. 19770809 200212 2 002**

Pembimbing II

**Nasron, S.T., M.T.
NIP. 19680822 199303 1 001**

Mengetahui,

**Ketua Jurusan
Teknik Elektro**

**Yudi Wianarko, S.T., M.T.
NIP. 19670511 199203 1 003**

**Ketua Program Studi Sarjana
Terapan Teknik Telekomunikasi**

**Sopian Soim, S.T., M.T.
NIP. 19710314 200112 1 001**

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini :

Nama : ARDELIA NIDYA AGUSTINA
NIM : 0613 4035 1618
Program Studi : Teknik Telekomunikasi
Jurusan : Teknik Elektro

Menyatakan dengan sesungguhnya bahwa Laporan Tugas Akhir yang telah saya buat ini dengan judul **“Pengamanan Dokumen Menggunakan Kombinasi Metode RSA (*Rivest Shamir Adleman*) dan *Vigenere Cipher*“** adalah benar hasil karya saya sendiri dan bukan merupakan duplikasi, serta tidak mengutip sebagian atau seluruhnya dari karya orang lain, kecuali yang telah disebutkan sumbernya.

Palembang, Agustus 2017

Penulis

ARDELIA NIDYA AGUSTINA

MOTTO DAN PERSEMBAHAN

"Karena sesungguhnya sesudah kesulitan ada kemudahan." (QS. Insyirah 5).

"Barang siapa yang keluar mencari ilmu dia ada di jalan Allah" (HR. Turmudzi)

kupersembahkan kepada :

- Allah SWT yang selalu mencurahkan nikmat dan kasih sayangnya .
- Kedua orang tuaku, Papaku Djoharsif Djanus dan Mamaku Zahara Madjid yang kucintai.
- Uni-uniku Armelia Rizky Hidayati,S.Pd., Arliza Nurul Ramadhani,A.md., dan Arfiani Ulfa Sari,S.E. yang telah memberikan dukungan dan do'a nya.
- Teman seperjuangan Telekomunikasi TEB POLSRI 2013.
- Para dosen dan staff di Teknik Telekomunikasi yang saya hormati.
- Almamaterku.

ABSTRAK

**PENGAMANAN DOKUMEN MENGGUNAKAN KOMBINASI METODE
RSA (*RIVEST SHAMIR ADLEMAN*) DAN *VIGENERE CIPHER*
(2017 : xvi + 76halaman + 62gambar + 9tabel + 9lampiran)**

ARDELIA NIDYA AGUSTINA

0613 4035 1618

JURUSAN TEKNIK ELEKTRO

**PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA**

Perkembangan teknologi masa kini berkembang pesat. Semakin hari semakin banyak pengguna yang mengakses internet. Salah satu akibat dari hal ini makin banyak nya penyadapan terhadap suatu dokumen yang bersifat rahasia. Sehingga apabila berbicara mengenai sebuah pengamanan pasti tidak akan jauh dari apa yang disebut kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Pada penelitian ini digunakan kombinasi dua metode. Yaitu metode RSA (*Rivest Shamir Adleman*) dan *Vigenere Cipher*. Dimana metode RSA ini mempunyai dua kunci yang berbeda pada proses enkripsi dan dekripsi. Dan *Vigenere Cipher* menggunakan kunci yang sama untuk proses enkripsi dan dekripsi nya. Pada penelitian ini, dilakukan suatu analisis dalam perspektif keamanan *file* yang bertujuan untuk mengamankan dokumen dari serangan-serangan yang dapat merusak *file*. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi menggunakan bahasa pemrograman *PHP* dan perangkat lunak sistem manajemen basis data *my SQL*. dua kombinasi metode yaitu metode RSA dan *Vigenere Cipher* termasuk dalam kategori metode yang aman dipakai untuk proses pengamanan dokumen.

Kata kunci: Kriptografi, RSA, *Vigenere Cipher*, *PHP*, *my SQL*

ABSTRACT

**SECURITY OF DOCUMENTS USING COMBINATIONS RSA METHOD
(RIVEST SHAMIR ADLEMAN) AND VIGENERE CIPHER
(2017 : xvi + 76pages + 62pictures + 9tables + 9appendixs)**

ARDELIA NIDYA AGUSTINA

0613 4035 1618

ELECTRICAL ENGINEERING

**PROGRAM OF STUDY IN APPLIED GRADUATION OF THE
TELECOMMUNICATION ENGINEERING
STATE POLYTECHNIC OF SRIWIJAYA**

The development of technology is now growing rapidly. Day by day users are accessing the internet. One result of this is the increasing number of tappers to a secret document. So when talking about a security would not be far from what is called cryptography. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication. In this study used a combination of the two methods. The method of RSA (Rivest Shamir Adleman) and Vigenere Cipher, Where the RSA method has two different keys in the encryption and decryption process. And Vigenere Cipher using the same key for encryption and decryption process it. In this study, carried out an analysis of the security perspectivefile which aims to secure documents from attacks that can damage file, The results of this study will be implemented in an application program using the programming language PHP and software management system database my SQL. two combination of methods is the method of RSA and Vigenere Cipher included in the category of safe methods used for the process of securing documents.

Keywords: cryptography, RSA, Vigenere Cipher, PHP, my SQL

KATA PENGANTAR

Puji syukur atas kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Laporan Tugas Akhir dengan judul “PENGAMANAN DOKUMEN MENGGUNAKAN KOMBINASI METODE RSA (*RIVEST SHAMIR ADLEMAN*) DAN *VIGENERE CIPHER*”. Laporan Tugas Akhir ini dibuat sebagai salah satu mata kuliah yang diberikan kepada mahasiswa jurusan Teknik Elektro program studi sarjana terapan Teknik Telekomunikasi.

Penulisan laporan tugas akhir ini tidak lepas dari arahan para pembimbing dan bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Bapak Yudi Wijanarko, S.T.,M.T. selaku Ketua Jurusan Teknik Elektro Politeknik Negeri Sriwijaya;
2. Bapak Herman Yani, S.T.,M.Eng. selaku Sekretaris Jurusan Teknik Elektro Politeknik Negeri Sriwijaya;
3. Bapak Sopian Soim, S.T.,M.T. selaku Ketua Program Studi Teknik Telekomunikasi DIV Politeknik Negeri Sriwijaya;
4. Ibu Aryanti, S.T., M.Kom. selaku Pembimbing 1, atas bimbingan, arahan, saran dan motivasi yang telah diberikan;
5. Bapak Nasron, S.T., M.T. selaku Pembimbing 2, atas bimbingan, saran dan motivasi yang telah diberikan;
6. Orang Tua serta seluruh keluarga tercinta yang telah memberikan semangat dan restu serta dukungan baik secara moril maupun materil;
7. Seluruh staf dan pengajar Teknik Elektro Program Studi Sarjana Terapan Teknik Telekomunikasi;
8. Teman-teman seperjuangan dalam menyelesaikan Laporan Tugas Akhir, terutama kelas 8 TEB Angkatan 2013;

Kami menyadari bahwa laporan tugas akhir ini masih banyak kesalahan dan kekurangan, untuk itu kritik dan saran yang bersifat membangun sehingga

laporan tugas akhir ini dapat memberikan manfaat dan dapat dikembangkan lebih lanjut lagi.

Palembang, Juli 2017

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
PERNYATAAN KEASLIAN	iii
MOTTO DAN PERSEMBAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	ix
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian	4
1.4. Manfaat Penelitian	4
1.5. Batasan Masalah	4
1.6. Metodologi Penulisan	4
1.7. Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA	7
2.1. Kriptografi	7
2.2. Sejarah Kriptografi.....	8
2.3. Istilah Pada Kriptografi	10
2.4. Macam-macam Algoritma Kriptografi	14
2.4.1. Algoritma Simetrik	14
2.4.1.1. Kelebihan dan Kekurangan Kunci Simetrik	15
2.4.2. Algoritma Asimetrik	16
2.4.2.1. Kelebihan dan Kekurangan Kunci Asimetrik	17
2.5. Kriptografi Klasik	17
2.6. Kriptografi <i>Hybird</i>	17
2.6.1. Proses Kriptografi <i>Hybird</i>	18
2.7. <i>Vigenere Ciphere</i>	19
2.8. <i>RSA (Rivest-Shamir-Adleman)</i>	20
2.9. Serangan Pada Kriptografi	21
2.10. <i>ASCII (American Standard Code For Information Interchange)</i>	22
2.11. <i>PHP (Personal Hypertext Preprocessor)</i>	25

2.12. <i>MySQL (My Structure Query Language)</i>	25
2.13. <i>XAMPP</i>	26
2.14. Data Flow Diagram.....	26
2.1.4.1. Diagram Konteks	28
2.1.4.2. Diagram Nol	28
2.15. <i>Entity Relationship Diagram (ERD)</i>	28
2.16. Perbandingan Metode.....	30
BAB III METODOLOGI PENELITIAN	31
3.1. Kerangka Penelitian	31
3.2. Perancangan Perangkat	32
3.2.1. Data <i>Flow</i> Diagram	33
3.2.1.1. Diagram Konteks	33
3.2.1.2. DFD Level 0	34
3.2.2. Entity Relationship Diagram (ERD)	35
3.2.3. Perancangan Tabel Database	36
3.3. Perancangan Tampilan Desain Aplikasi	38
3.3.1. Perancangan Desain <i>Interface</i>	38
3.3.2. Perancangan Desain Tampilan Visi dan Misi.....	39
3.3.3. Perancangan Desain Tampilan Sejarah.....	39
3.3.4. Perancangan Desain Tampilan Denah Lokasi	40
3.3.5. Perancangan Desain Tampilan <i>login</i>	40
3.3.6. Perancangan Desain Tampilan Data Dosen	41
3.3.7. Perancangan Desain Tampilan Daftar Mahasiswa.....	42
3.3.8. Perancangan Desain Tampilan Daftar Enkripsi	42
3.3.9. Perancangan Desain Tampilan Riwayat <i>Upload File</i>	43
3.3.10. Perancangan Desain Tampilan Riwayat Unduhan.....	44
3.3.11. Perancangan Desain Tampilan Profil Dosen	44
3.3.12. Perancangan Desain Tampilan Daftar <i>File</i>	45
3.3.13. Perancangan Desain Tampilan <i>Form</i> Enkripsi	46
3.3.14. Perancangan Desain Tampilan Materi Perkuliahan	46
3.3.15. Perancangan Desain Tampilan Profil Mahasiswa	47
3.3.16. Perancangan Desain Tampilan Daftar <i>File</i>	48
3.3.17. Perancangan Desain Tampilan Materi Perkuliahan	49
3.4. Perancangan Algoritma Pada Aplikasi.....	49
3.5. Persiapan Data	54
3.6. Pengembangan Metode	54
3.7. Tes Kinerja Sistem	55
BAB IV HASIL DAN PEMBAHASAN	56
4.1. Tampilan Aplikasi Secara Keseluruhan	56

4.1.1. Tampilan Awal	56
4.1.2. Tampilan Visi dan Misi	57
4.1.3. Tampilan Sejarah	57
4.1.4. Tampilan Denah Lokasi	58
4.1.5. Tampilan <i>Login</i>	58
4.1.6. Tampilan <i>Login</i> admin	59
4.1.6.1. Tampilan Daftar Dosen	59
4.1.6.2. Tampilan Daftar Mahasiswa	60
4.1.6.3. Tampilan Daftar Enkripsi	61
4.1.6.4. Tampilan Riwayat Download	61
4.1.7. Tampilan <i>Login</i> Dosen	62
4.1.7.1. Tampilan Profil Dosen	62
4.1.7.2. Tampilan Upload <i>File</i>	63
4.1.7.3. Tampilan Materi Perkuliahan	63
4.1.7.4. Tampilan Riwayat <i>Upload File</i>	64
4.1.8. Tampilan <i>Login</i> Mahasiswa	64
4.1.8.1. Tampilan Profil Mahasiswa	64
4.1.8.2. Tampilan Daftar <i>File</i>	65
4.1.8.3. Tampilan Materi Perkuliahan	66
4.1.8.4. Tampilan Riwayat Unduhan	66
4.2. Pengujian Proses Enkripsi dan Dekripsi	67
4.3. Analisis	72
4.4. Pengujian Waktu Proses Enkripsi dan Dekripsi	75
BAB V KESIMPULAN DAN SARAN	76
5.1. Kesimpulan	76
5.2. Saran	76

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

	Halaman
2.1 Tulisan yang menggunakan <i>hieroglyph</i>	9
2.2 Proses Enkripsi dan Dekripsi	14
2.3 Proses Enkripsi dan Dekripsi Algoritma Simetrik	15
2.4 Proses Enkripsi dan Dekripsi Algoritma Asimetrik.....	17
2.5 Tabel ASCII 0-255 Karakter	24
2.6 Contoh Bentuk Diagram Konteks	28
2.7 Contoh Bentuk Diagram Nol	28
3.1 Diagram Perancangan Secara Keseluruhan	31
3.2 <i>Flowchart</i> Perancangan Pengamanan Dokumen	32
3.3 Diagram Konteks Pengamanan Dokumen	33
3.4 DFD Level 0 Perancangan Pengamanan Dokumen	34
3.5 <i>Entity Relationship Diagram (ERD)</i> Pengamanan Dokumen	35
3.6 Desain <i>Interface</i>	34
3.7 Desain Tampilan Visi & Misi	39
3.8 Desain Tampilan Sejarah	39
3.9 Desain Tampilan Denah Lokasi	40
3.10 Desain Tampilan <i>Login</i>	41
3.11 Desain Tampilan Data Dosen.....	41
3.12 Desain Tampilan Data Mahasiswa.....	42
3.13 Desain Tampilan Daftar Enkripsi.....	43
3.14 Desain Tampilan Riwayat <i>Upload</i>	43
3.15 Desain Tampilan Riwayat Unduhan	44
3.16 Desain Tampilan Profil Dosen	45
3.17 Desain Tampilan Daftar Enkripsi.....	45
3.18 Desain Tampilan <i>Form</i> Enkripsi.....	46
3.19 Desain Tampilan Materi Perkuliahan.....	47
3.20 Desain Tampilan Profil Mahasiswa	47
3.21 Desain Tampilan Daftar <i>File</i>	48
3.22 Desain Tampilan <i>Input Password</i> Deskripsi.....	48
3.23 Desain Tampilan Materi Perkuliahan.....	49
4.1 Tampilan Awal.....	56
4.2 Tampilan Visi & Misi	57
4.3 Tampilan Sejarah	57
4.4 Tampilan Denah Lokasi	58
4.5 Tampilan <i>Login</i>	58

4.6 Tampilan Login Admin.....	59
4.7 Tampilan Daftar Dosen.....	60
4.8 Tampilan Daftar Mahasiswa.....	60
4.9 Tampilan Riwayat <i>Upload File</i>	61
4.10 Tampilan Riwayat <i>Download</i>	61
4.11 Tampilan <i>Login</i> Dosen.....	62
4.12 Tampilan Profil Dosen.....	62
4.13 Tampilan <i>Upload File</i>	63
4.14 Tampilan Materi Perkuliahan.....	63
4.15 Tampilan Riwayat <i>Download</i>	64
4.16 Tampilan Profil Mahasiswa.....	65
4.17 Tampilan Daftar <i>File</i>	65
4.18 Tampilan Materi Perkuliahan.....	66
4.19 Tampilan Riwayat Unduhan.....	66
4.20 Tampilan <i>Login</i> Dosen.....	67
4.21 Tampilan <i>Upload</i> Untuk Proses Enkripsi.....	68
4.22 Tampilan Proses Dari Enkripsi.....	68
4.23 Tampilan <i>File</i> Yang Berhasil Dienkripsi.....	69
4.24 Tampilan <i>Login</i> Mahasiswa.....	69
4.25 Tampilan Daftar <i>File</i>	70
4.26 Tampilan <i>Input Password</i> Proses Deskripsi.....	70
4.27 Tampilan <i>File</i> Tidak Dapat Terbuka.....	71
4.28 Tampilan <i>Input Password</i> Proses Deskripsi.....	71
4.29 Tampilan <i>File</i> Berhasil Dideskripsi.....	72
4.30 Tampilan <i>File</i> “data2.docx Dalam Heksadesimal”.....	73
4.31 Tampilan <i>File</i> “data2(1).docx Dalam Heksadesimal”.....	73
4.32 Tampilan <i>File</i> “data2(2).docx Dalam Heksadesimal”.....	74

DAFTAR TABEL

	Halaman
2.1 Perbandingan Metode	30
3.1 Tabel Dekripsi.....	36
3.2 Tabel Dosen	36
3.3 Tabel Enkripsi	36
3.4 Tabel Mahasiswa	37
3.5 Tabel Materi Perkuliahan	38
4.1 Pengujian Waktu Proses Enkripsi dan Dekripsi	76

DAFTAR LAMPIRAN

- Lampiran 1** Lembar Rekomendasi
- Lampiran 2** Lembar Kesepakatan Bimbingan TA Pembimbing I
- Lampiran 3** Lembar Kesepakatan Bimbingan TA Pembimbing II
- Lampiran 4** Lembar Konsultasi Pembimbing I
- Lampiran 5** Lembar Konsultasi Pembimbing II
- Lampiran 6** Surat Pernyataan Pengumpulan Draft Jurnal (TA)
- Lampiran 7** Lembar Daftar Riwayat Hidup
- Lampiran 8** Lembar LOA
- Lampiran 9** Pelaksanaan Revisi Tugas Akhir