



**Pengaplikasian Algoritma Kriptografi RSA Untuk Enkripsi File Document
dan Algoritma Transposisi Kolom Untuk Enkripsi Kunci Private Dengan
PHP**

Andreas Febrian Idris

41514310027

UNIVERSITAS
MERCU BUANA

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2018**



**Pengaplikasian Algoritma Kriptografi RSA Untuk Enkripsi File Document
dan Algoritma Transposisi Kolom Untuk Enkripsi Kunci Private Dengan
PHP**

Laporan Tugas Akhir

Diajukan Untuk Melengkapi Persyaratan
Menyelesaikan Gelar Sarjana Komputer

Disusun oleh :

Andreas Febrian Idris

41514310027

UNIVERSITAS
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS MERCU BUANA

JAKARTA

2018

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41514310027

Nama : Andreas Febrian Idris

Judul Tugas Akhir : Pengaplikasian Algoritma Kriptografi RSA Untuk Enkripsi
File Document dan Algoritma Transposisi Kolom Untuk
Enkripsi Kunci Private Dengan PHP

Menyatakan bahwa Tugas Akhir dengan judul yang tersebut diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan didalam Laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta 28 Juli 2018
METERAI
TEMPEL
992ACAEF905407642
6000
ENAM RIBU RUPIAH
Andreas Febrian Idris

LEMBAR PENGESAHAN

Nama : Andreas Febrian Idris
NIM : 41514310027
Jurusan : Teknik Informatika
Fakultas : Ilmu Komputer
Judul : Pengaplikasian Algoritma Kriptografi RSA Untuk Enkripsi
File Document dan Algoritma Transposisi Kolom Untuk
Enkripsi Kunci Private Dengan PHP

Jakarta, 28 Juli 2018

Disetujui dan diterima oleh,

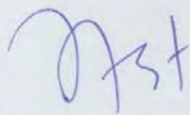


UNIVERSITAS

Adi Hartanto, ST, M. Kom

Dosen Pembimbing

MERCU BUANA



Desi Ramayanti, S.Kom., M.T.

Kaprodi Teknik Informatika



Sri Dianing Asri, ST., M.Kom

Koordinator Tugas Akhir

LEMBAR PERSETUJUAN SIDANG

Yang bertanda tangan di bawah ini menyatakan bahwa skripsi dari mahasiswa :

Nama Mahasiswa : Andreas Febrian Idris
NIM : 41514310027
Fakultas : Ilmu Komputer
Program Studi : Teknik Informatika
Judul : Pengaplikasian Algoritma Kriptografi RSA Untuk
Enkripsi File Document dan Algoritma Transposisi
Kolom Untuk Enkripsi Kunci Private Dengan PHP



UNIVERSITAS

Jakarta, 29 Juni 2018

Disetujui dan diterima untuk di sidangkan,
MERCU BUANA

Aq. Hartanto, ST. M.Kom

Dosen Pembimbing

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga penulis dapat menyelesaikan Karya Tulis Ilmiah ini yang berjudul "**Pengaplikasian Algoritma Kriptografi RSA Untuk Enkripsi File Document dan Algoritma Transposisi Kolom Untuk Enkripsi Kunci Private Dengan PHP**"

Penulisan penelitian ini bertujuan untuk memenuhi syarat kelulusan pada Program Studi Teknik Informatika Universitas Mercu Buana. Karya tulis ini terwujud berkat bantuan berbagai pihak, karena itu penulis mengucapkan terima kasih kepada:

1. Kepada Tuhan Yesus Kristus yang telah memampukan saya dalam menyelesaikan penulisan penelitian ini.
2. Kepada kedua orang tua saya yang selalu mendoakan dan menasehati saya, sehingga saya dapat boleh sampai pada tahap Tugas Akhir ini.
3. Kepada Ka Imel dan Indira selaku kakak dan adik saya yang selalu menasehati saya untuk selalu semangat dalam menyelesaikan penulisan penelitian ini.
4. Kepada Bapak Adi Hartanto, ST. M.Kom, sebagai Dosen Pembimbing Tugas Akhir saya yang membimbing saya untuk menyelesaikan penulisan penelitian ini.
5. Kepada Bapak Muhammad Rifqi, S. Kom, M. Kom sebagai Dosen Kriptografi saya yang memberikan masukan dan saran mengenai ilmu-ilmu dalam dunia kriptografi.
6. Kepada seluruh Dosen Teknik Informatika Universitas Mercu Buana Kampus D (Kranggan) yang memberikan ilmu-ilmu selama saya berkuliah.
7. Kepada seluruh teman-teman saya yaitu Teknik Informatika Angkatan 25(TI-25) yang berjuang bersama dalam menyelesaikan tugas akhir ini.

Bekasi, 30 Juni 2018

Andreas Febrian Idris

DAFTAR ISI

ABSTRAKSI.....	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
LEMBAR PERNYATAAN	iv
LEMBAR PERSETUJUAN SIDANG	v
LEMBAR PENGESAHAN SIDANG	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xi
DEFINISI	xii
BAB 1. PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Permasalahan.....	2
1.3. Tujuan & Manfaat Penelitian	2
1.3.1 Tujuan Penelitian	2
1.3.2 Manfaat Penelitian	3
1.4. Ruang Lingkup & Batasan Penelitian	3
1.5. Sistematika Penulisan Laporan.....	3
1.5.1 Pendahuluan	3
1.5.2 Landasan Teori.....	3
1.5.3 Analisis Sistem.....	4
1.5.4 Perancangan Sistem	4
1.5.5 Implementasi Dan Testing	4
1.5.6 Penutup.....	4
1.6. Metodologi Penelitian.....	4

BAB 2.	LANDASAN TEORI.....	6
2.1.	Perolehan Informasi (IR) Berbasis Konteks.....	6
2.2.	Interaksi Antar Obyek	8
2.2.1	Aplikasi	8
2.2.2	Kriptografi.....	9
2.2.3	Algoritma RSA (<i>Rivest-Shamir-Adleman</i>).....	13
2.2.4	Algoritma Transposisi Kolom.....	15
2.2.5	PHP	16
BAB 3.	ANALISA SISTEM.....	18
3.1.	Analisa Sistem.....	18
3.2.	Analisa Kebutuhan	18
3.2.1	Analisa Perangkat Keras (<i>Hardware</i>).....	18
3.2.2	Analisa Perangkat Lunak (<i>Software</i>)	19
3.2.3	Analisa Perangkat Manusia (<i>Brainware</i>).....	19
BAB 4.	PERANCANGAN	20
4.1.	Perancangan Algoritma	20
4.1.1	Algoritma Form Enkripsi	20
4.1.2	Algoritma Proses Enkripsi	21
4.1.3	Algoritma Proses Enkripsi Kunci Kombinasi.....	21
4.1.4	Algoritma Form Dekripsi.....	22
4.1.5	Algoritma Proses Dekripsi Kunci Kombinasi.....	23
4.1.6	Algoritma Proses Enkripsi	24
4.2.	Perancangan Sistem.....	24
4.2.1	Use Case Diagram.....	24
4.2.2	Activity Diagram.....	26
4.2.3	Sequence Diagram.....	27
4.3.	Struktur Menu dan Rancangan User Interface	29

4.3.1	Rancangan Tampilan Halaman Awal.....	29
4.3.2	Rancangan Tampilan Form Enkripsi	29
4.3.3	Rancangan Tampilan Form Dekripsi	30
BAB 5.	IMPLEMENTASI DAN PENGUJIAN	31
5.1.	Lingkungan Implementasi	31
5.1.1	Perangkat Keras	31
5.1.2	Perangkat Lunak Platform	31
5.2.	Hasil Implementasi.....	32
5.2.1	Tampilan Halaman Awal	32
5.2.2	Tampilan Halaman Form Enkripsi.....	32
5.2.3	Tampilan Halaman Form Dekripsi.....	35
5.3.	Hasil Pengujian.....	39
5.3.1	Skenario Uji Coba.....	39
5.3.2	Hasil Uji Coba.....	41
BAB 6.	PENUTUP	49
6.1.	Kesimpulan.....	49
6.2.	Saran	49
DAFTAR PUSTAKA		xiii
LAMPIRAN.....		xv

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi Pada Algoritma Simetris.....	10
Gambar 2.2 Proses Enkripsi dan Dekripsi Pada Algoritma Asimetris	11
Gambar 2.3 Proses Enkripsi dan Deskripsi Pada Algoritma RSA.....	14
Gambar 2.4 Proses Enkripsi Dengan Algoritma Transposisi Kolom	15
Gambar 3.1 Flowchart Kerangka Umum Aplikasi Enkripsi dan Dekripsi	18
Gambar 4.1 Use Case Aplikasi Enkripsi dan Dekripsi	25
Gambar 4.2 Activity Diagram Enkripsi	26
Gambar 4.3 Activity Diagram Dekripsi	27
Gambar 4.4 Sequence Diagram Enkripsi	28
Gambar 4.5 Sequence Diagram Dekripsi.....	28
Gambar 4.6 Halaman Awal.....	29
Gambar 4.7 Form Enkripsi.....	29
Gambar 4.8 Form Dekripsi	30
Gambar 5.1 Halaman Awal.....	32
Gambar 5.2 Form Enkripsi Sebelum Proses Enkripsi.....	33
Gambar 5.3 Form Enkripsi Saat User Mengunggah File.....	33
Gambar 5.4 Jika Extantion File Tidak Diizinkan	34
Gambar 5.5 Jika Ukuran Byte File > 2MB	34
Gambar 5.6 Form Enkripsi Saat Proses Enkripsi.....	35
Gambar 5.7 Form Enkripsi Setelah Proses Enkripsi Selesai	35
Gambar 5.8 Gambar Form Dekripsi Sebelum Proses Dekripsi	36
Gambar 5.9 Form Dekripsi Saat User Mengunggah File.....	36
Gambar 5.10 Jika Extantion File Tidak Diizinkan.....	37
Gambar 5.11 Jika Ukuran Byte File > 2MB	37
Gambar 5.12 Pesan Jika Kunci Kombinasi dan Nama Penerima Tidak Cocok....	38
Gambar 5.13 Form Enkripsi Saat Proses Enkripsi.....	38
Gambar 5.14 Jika Proses Dekripsi Selesai.....	39