

TUGAS AKHIR

**IMPLEMENTASI *DOUBLE ENCRYPTION* DAN
OPENSSL LIBRARY PADA SISTEM KEAMANAN
BASIS DATA BERBASIS ENKRIPSI AES-256 DAN
RSA**



DIMAS GUMERANG RYANDIKA

19102004

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2023**

TUGAS AKHIR

**IMPLEMENTASI *DOUBLE ENCRYPTION* DAN
OPENSSL LIBRARY PADA SISTEM KEAMANAN
BASIS DATA BERBASIS ENKRIPSI AES-256 DAN
RSA**

**IMPLEMENTATION OF DOUBLE ENCRYPTION
AND OPENSSL LIBRARY IN AES-256 AND RSA-
BASED DATABASE SECURITY SYSTEM**

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer



DIMAS GUMERANG RYANDIKA

19102004

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2023**

LEMBAR PERSETUJUAN PEMBIMBING

**IMPLEMENTASI *DOUBLE ENCRYPTION* DAN
OPENSSL LIBRARY PADA SISTEM KEAMANAN
BASIS DATA BERBASIS ENKRIPSI AES-256 DAN
RSA**

**IMPLEMENTATION OF DOUBLE ENCRYPTION
AND OPENSSL LIBRARY IN AES-256 AND RSA-
BASED DATABASE SECURITY SYSTEM**

Dipersiapkan dan Disusun oleh

DIMAS GUMERANG RYANDIKA

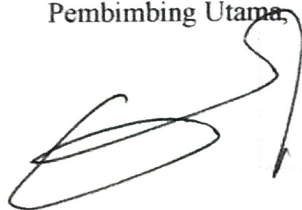
19102004

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 31 Juli 2023

Pembimbing Utama,



Wahyu Adi Prabowo, S.Kom., M.B.A.,
M.Kom.
NIDN. 0613038503

Pembimbing Pendamping,



Arif Wirawan Muhammad, S.Kom.,
M.Kom.
NIDN. 0601098701

LEMBAR PENGESAHAN

**IMPLEMENTASI DOUBLE ENCRYPTION DAN
OPENSSL LIBRARY PADA SISTEM KEAMANAN
BASIS DATA BERBASIS ENKRIPSI AES-256 DAN
RSA**

**IMPLEMENTATION OF DOUBLE ENCRYPTION
AND OPENSSL LIBRARY IN AES-256 AND RSA-
BASED DATABASE SECURITY SYSTEM**

Disusun Oleh

DIMAS GUMERANG RYANDIKA

19102004

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas

Akhir Pada 21 Agustus 2023

Penguji I,




Bitu Parga Zen, S.Kom., M.Han.
NIDN. 0603089202

Penguji II,



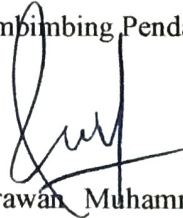
Mega Pranata S.Pd., M.Kom.
NIDN. 061069301

Pembimbing Utama,



Wahyu Adi Prabowo, S.Kom., M.B.A.,
M.Kom.
NIDN. 0613038503

Pembimbing Pendamping,



Arif Wirawan Muhammad, S.Kom.,
M.Kom.
NIDN. 0601098701

Dekan,



Auliya Burhanuddin, S.Si., M.Kom.
NIK. 9820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan dibawah ini,

Nama Mahasiswa : Dimas Gumerang Ryandika
NIM : 19102004
Program Studi : SI Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:
**IMPLEMENTASI DOUBLE ENCRYPTION DAN OPENSLL LIBRARY
PADA SISTEM KEAMANAN BASIS DATA BERBASIS ENKRIPSI AES-
256 DAN RSA**

Dosen Pembimbing Utama : Wahyu Adi Prabowo, S.Kom., M.B.A.,
M.Kom.

Dosen Pembimbing Pendamping : Arif Wirawan Muhammad, S.Kom.,
M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing.
3. Dalam Karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima Sanksi Akademik dengan pencabutan gelar yang sudah diperoleh serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Purwokerto, 25 Agustus 2023

Yang Menyatakan,
(materai 10000 dan tanda tangan)



(Dimas Gumerang Ryandika)

KATA PENGANTAR

Dengan mengucapkan puji syukur kepada Allah SWT yang telah melimpahkan rahmat, berkah serta petunjuknya sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “**Implementasi *Double Encryption* Dan *Openssl Library* Pada Sistem Keamanan Basis Data Berbasis Enkripsi AES-256 Dan RSA**” sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) Program Sarjana Program Studi Teknik Informatika Fakultas Informatika Institut Teknologi Telkom Purwokerto. Pada prosesnya, penulis menyadari betapa besarnya dukungan, bantuan, bimbingan, serta doa dan harapan dari berbagai pihak selama proses penyusunan tugas akhir ini. Pada kesempatan ini, penulis menyampaikan terimakasih sebesar-besarnya kepada :

1. Allah SWT Tuhan Yang Maha Esa atas petunjuk dan pertolongannya dalam proses penyusunan tugas akhir ini.
2. Kedua orang tua saya, Bapak Sanrukyat dan (Almh.) Ibu Khotimah yang tidak henti-hentinya memberikan dukungan serta doa selama penyusunan tugas akhir ini.
3. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T. selaku Rektor Institut Teknologi Telkom Purwokerto.
4. Bapak Auliya Burhanuddin, S.Si., M.Kom. selaku Dekan Fakultas Informatika.
5. Ibu Amalia Beladonna Arifa, S.Pd., M.Cs. selaku Kepala Program Studi Teknik Informatika.
6. Bapak Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom. selaku dosen pembimbing utama yang telah sepenuh hati membimbing penulis selama penyusunan tugas akhir ini.
7. Bapak Arif Wirawan Muhammad, S.Kom., M.Kom. selaku dosen pembimbing pendamping.
8. Bapak Yoso Adi Setyoko, S.T., M.T. selaku dosen wali yang telah mendidik, membimbing dan membantu penulis selama menempuh masa studi di Institut Teknologi Telkom Purwokerto.

9. Seluruh staff dan tenaga pengajar Fakultas Informatika Institut Teknologi Telkom Purwokerto yang telah memberikan ilmu pengetahuan yang tidak ternilai selama penulis menempuh dan menyelesaikan studi di Fakultas Informatika Institut Teknologi Telkom Purwokerto.
10. Jajaran, staff dan semua elemen Kemenristekdikti dan Kemendikbud yang telah membantu saya dalam menyelesaikan program Sarjana Institut Teknologi Telkom Purwokerto melalui program beasiswa Bidikmisi.
11. Saudara Aziz Tri Nugroho dan Indra Agrisetya selaku teman kelas yang telah mendukung dan membantu penulis selama menempuh dan menyelesaikan masa studi di Institut Teknologi Telkom Purwokerto.
12. Saudara Teguh Rijanandi selaku teman almamater SLTA yang telah membantu penulis selama penyusunan proyek tugas akhir ini.
13. Saudara Tangguh Rizky Nurwendys yang telah memberikan informasi terkait adanya kuota beasiswa kepada penulis saat mendaftar di Institut Teknologi Telkom Purwokerto pada 2019.
14. Segenap pihak yang tidak dapat penulis tuliskan satu persatu yang telah membantu penulis selama menempuh pendidikan sarjana di Institut Teknologi Telkom Purwokerto.

Penulis menyadari dan memohon maaf sebesar-besarnya apabila masih terdapat banyak kekurangan dalam menyusun tugas akhir ini. Penulis berharap agar tugas akhir ini dapat bermanfaat untuk pembaca serta dapat menjadi referensi untuk penelitian lanjutan berikutnya yang lebih baik. Akhir kata, penulis mengharapkan masukan serta kritik dan juga saran dari berbagai pihak untuk kesempurnaan tugas akhir ini. Terimakasih.

Purwokerto, 25 Agustus 2023

Penulis

(Dimas Gumerang Ryandika)

DAFTAR ISI

HALAMAN COVER	i
LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PENGESAHAN	iii
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR ISTILAH	xii
DAFTAR SINGKATAN	xiii
DAFTAR LAMPIRAN	xiv
ABSTRAK	xv
ABSTRACT	xvi
BAB I : PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah.....	2
1.3 Pertanyaan Penelitian	2
1.4 Tujuan Penelitian.....	3
1.5 Batasan Masalah.....	3
1.6 Manfaat Penelitian.....	3
BAB II : TINJAUAN PUSTAKA DAN LANDASAN TEORI	4
2.1 Tinjauan Pustaka	4
2.2 Landasan Teori	16
2.2.1 <i>Database</i>	16
2.2.2 Algoritma <i>Advanced Encryption Standard (AES)</i>	18
2.2.3 Algoritma Rivest Shamir Adleman (RSA)	20
2.2.4 <i>Web Server</i>	21
2.2.5 Layanan Web	21
2.2.6 Serangan <i>SQL Injection</i>	22
2.2.7 <i>Web Hosting</i>	22

2.2.8	PHP	22
2.2.9	<i>Openssl Library</i>	23
BAB III : METODOLOGI PENELITIAN		24
3.1	Objek dan Subjek Penelitian	24
3.1.1	Objek Penelitian	24
3.1.2	Subjek Penelitian.....	24
3.2	Alat dan Bahan Penelitian	24
3.2.1	Alat Penelitian	24
3.2.2	Bahan Penelitian.....	25
3.3	Metodologi Penelitian	26
3.3.1	Pemodelan Sistem	27
3.3.2	Perancangan Model AES-256.....	28
3.3.3	Perancangan Model RSA	30
3.3.4	Pengintegrasian Sistem	32
3.3.5	Pengujian Sistem.....	34
3.3.6	Penarikan Kesimpulan	35
BAB IV : HASIL DAN PEMBAHASAN		37
4.1	Hasil.....	37
4.1.1	Model Sistem	37
4.1.2	Model AES-256	39
4.1.3	Model RSA	41
4.1.4	Integrasi Sistem.....	45
4.1.5	Pengujian Sistem.....	47
4.2	Pembahasan	55
BAB V : KESIMPULAN DAN SARAN.....		56
5.1	Kesimpulan.....	56
5.2	Saran	56
DAFTAR PUSTAKA		58
LAMPIRAN.....		64

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	7
Tabel 2. 2 Tabel Perbandingan Enkripsi AES Berdasarkan Ukuran Bit.....	18
Tabel 3. 1 Spesifikasi Web Hosting	24
Tabel 3. 2 Spesifikasi perangkat tester.....	25
Tabel 3. 3 Konfigurasi Web Hosting	27
Tabel 3. 4 Konfigurasi tabel target.....	28

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Database	17
Gambar 2. 2 Alur Kerja Algoritma AES.....	18
Gambar 2. 3 Diagram Skema Enkripsi AES 256.....	19
Gambar 2. 4 Alur Algoritma RSA	20
Gambar 2. 5 Cara Kerja Layanan Web	21
Gambar 3. 1 Metodologi Penelitian	26
Gambar 3. 2 Desain Arsitektur Sistem.....	27
Gambar 3. 3 Pemodelan Enkripsi AES-256 CBC.....	29
Gambar 3. 4 Pemodelan Dekripsi AES-256	30
Gambar 3. 5 Pemodelan Enkripsi RSA.....	31
Gambar 3. 6 Pemodelan Dekripsi RSA.....	32
Gambar 3. 7 Integrasi Model Enkripsi Ke Dalam Sistem.....	33
Gambar 3. 8 Integrasi Model Dekripsi Ke Dalam Sistem	34
Gambar 3. 9 Skema Alur Pengujian Sistem.....	35
Gambar 4. 1 Tampilan Sistem.....	37
Gambar 4. 2 Skema Model Database	37
Gambar 4. 3 Halaman Add Data	38
Gambar 4. 4 Halaman Edit Data	39
Gambar 4. 5 Model Enkripsi AES-256.....	39
Gambar 4. 6 Model Dekripsi AES	40
Gambar 4. 7 Penggabungan Model Enkripsi RSA dan AES-256.....	40
Gambar 4. 8 Proses Pembuatan Private Key dan Public Key	41
Gambar 4. 10 Isi dari Public Key	42
Gambar 4. 11 Model Enkripsi RSA	42
Gambar 4. 12 Isi dari Private Key.....	43
Gambar 4. 13 Penggabungan Model Enkripsi AES-256 dan RSA.....	44
Gambar 4. 14 Model Dekripsi RSA.....	45
Gambar 4. 15 Integrasi Model Enkripsi Pada Create Data	45
Gambar 4. 16 Integrasi Model Enkripsi Pada Update Data.....	46

Gambar 4. 17 Integrasi Model Dekripsi Pada Halaman Index	47
Gambar 4. 18 Entry Data Pengujian	48
Gambar 4. 19 Data Bahan Pengujian Pada PHPMyAdmin	48
Gambar 4. 20 Pengecekan Error SQL Syntax Pada URL.....	49
Gambar 4. 21 Pengujian Tautan Menggunakan SQL Map	50
Gambar 4. 22 Hasil Pengujian URL Menggunakan SQL Map.....	50
Gambar 4. 23 Pencarian Database Menggunakan SQL Map.....	51
Gambar 4. 24 Pencarian Tabel Menggunakan SQL Map	52
Gambar 4. 25 Perintah Pencarian Kolom Menggunakan SQL Map.....	53
Gambar 4. 26 Input Perintah Dumping Data Menggunakan SQL Map.....	54
Gambar 4. 27 Hasil Dumping Data Menggunakan SQL Map.....	54
Gambar Lampiran 1. 1 Struktur Tabel Siswa.....	64
Gambar Lampiran 1. 2 Isi tabel “siswa”	64
Gambar Lampiran 2. 1 Isi kode Add Data.php bagian satu	65
Gambar Lampiran 2. 2 Isi kode Add Data.php bagian dua.....	66
Gambar Lampiran 2. 3 Isi kode ubah.php bagian satu.....	67
Gambar Lampiran 2. 4 Isi kode ubah.php bagian satu.....	68
Gambar Lampiran 2. 5 Isi kode index.php bagian satu.....	69
Gambar Lampiran 2. 6 Isi kode index.php bagian dua	70
Gambar Lampiran 2. 7 Isi kode index.php bagian tiga	71
Gambar Lampiran 2. 8 Isi kode hapus.php	72
Gambar Lampiran 2. 9 Kode fungsi query.....	72
Gambar Lampiran 2. 10 Kode fungsi “tambah”	73
Gambar Lampiran 2. 11 Kode fungsi “hapus”	73
Gambar Lampiran 2. 12 Kode fungsi “ubah”	73
Gambar Lampiran 3. 1 Struktur sistem tersimpan pada web hosting	74

DAFTAR ISTILAH

Database	: Tempat penyimpanan data sebuah sistem pada jaringan internet.
SQL Injection	: Serangan pada database dengan manipulasi celah query SQL.
AES	: Metode kriptografi simetris pengembangan lanjutan dari DES.
RSA	: Metode kriptografi asimetris dengan memanfaatkan kunci publik dan privat.
OpenSSL	: Aplikasi open source untuk berbasis protokol Secure Socket Layer (SSL) dan Transport Layer Security (TLS).
Enkripsi	: Pengacakan data dengan metode perhitungan matematika tertentu.
Dekripsi	: Pengembalian data yang telah teracak menjadi teks normal.
Query	: Perintah dalam aplikasi database untuk mendapatkan informasi tertentu.
PHP	: Bahasa pemrograman <i>server scripting</i> yang bersifat open source.
Plaintext	: Istilah kriptografi untuk teks normal yang belum tersandi.
Ciphertext	: Teks tersandi dengan metode pengacakan/enkripsi tertentu.
Web Hosting	: Layanan yang untuk menyimpan file dan data suatu website.
Server	: Sistem komputer yang menjalankan jenis layanan tertentu.

DAFTAR SINGKATAN

AES	: Advanced Encryption Standard
RSA	: Rivest Shamir Adleman
SQL	: Structured Query Language
PHP	: Hypertext Preprocessor
URL	: Uniform Resource Locator
CBC	: Cipher Block Chaining
SSL	: Secure Socket Layer

DAFTAR LAMPIRAN

Lampiran 1. Data Pengujian.....	64
Lampiran 2. Fungsi CRUD	64
Lampiran 3. Struktur Sistem	73