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,

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

Penguji II,

Mega Pranata S.Pd., M.Kom.
NIDN. 061[illegible]069301

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,

Aulia Burhanuddin, S.Si., M.Kom.
NIK [illegible]9820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan dibawah ini,

Nama Mahasiswa	**: Dimas Gumerang Ryandika**
NIM	**: 19102004**
Program Studi	**: S1 Teknik Informatika**

Menyatakan bahwa Tugas Akhir dengan judul berikut:
IMPLEMENTASI DOUBLE ENCRYPTION DAN OPENSSL 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 Beladinna 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

DAFTAR TABEL

DAFTAR GAMBAR

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 *server scripting* 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