TUGAS AKHIR

PERANCANGAN SISTEM KEAMANAN DATA MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

AZIZ TRI NUGROHO

19102253

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS INFORMATIKA

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

2023

TUGAS AKHIR

PERANCANGAN SISTEM KEAMANAN DATA MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

DATA SECURITY SYSTEM DESIGN BASED ON MERKLE–HELLMAN KNAPSACK ENCRYPTION AND ADVANCED ENCRYPTION STANDARD (AES)

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

AZIZ TRI NUGROHO

19102253

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS INFORMATIKA

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

2023

LEMBAR PERSETUJUAN PEMBIMBING

PERANCANGAN SISTEM KEAMANAN DATA MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

DATA SECURITY SYSTEM DESIGN BASED ON MERKLE–HELLMAN KNAPSACK ENCRYPTION AND ADVANCED ENCRYPTION STANDARD (AES)

Dipersiapkan dan Disusun oleh

AZIZ TRI NUGROHO

19102253

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 7 Agustus 2023

Pembimbing Utama,	Pembimbing Pendamping,
Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom.	Arif Wirawan Muhammad, S.Kom., M.Kom.
NIDN. 0613038503	NIDN. 0601098701

LEMBAR PENGESAHAN

PERANCANGAN SISTEM KEAMANAN DATA MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

DATA SECURITY SYSTEM DESIGN USING MERKLE–HELLMAN KNAPSACK ENCRYPTION AND ADVANCED ENCRYPTION STANDARD (AES)

Disusun Oleh
AZIZ TRI NUGROHO
19102253

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,

Cahyo Prihantoro, S.Kom., M.Eng.

NIDN. 0221019002

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. 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan dibawah ini,

Nama Mahasiswa : Aziz Tri Nugroho
NIM : 19102253
Program Studi : S1 Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:

PERANCANGAN SISTEM KEAMANAN DATA MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

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, 7 Agustus 2023

Yang

(Aziz tri Nugroho)

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 **"Perancangan Sistem Keamanan Data Menggunakan Enkripsi Merkle-hellman Knapsack dan Advancce Encryption Standard (AES)"** 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 :

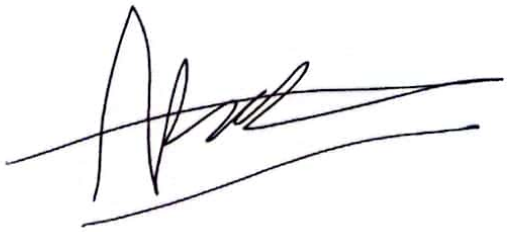
1. Allah SWT atas petunjuk dan pertolongannya dalam proses penyusunan tugas akhir ini.
2. Kedua orang tua saya, (Almarhum) Dartim Al Ari Wijaya dan Tasirah yang tidak henti-hentinya memberikan dukungan serta doa selama penyusunan tugas akhir ini.
3. Ibu Dr. Tenia Wahyuningrum, S.Kom., M.T Selaku Rektor 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 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.
7. 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.
8. Bapak Arif Wirawan Muhammad, S.Kom., M.Kom. selaku dosen pembimbing pendamping.

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. Saudara Dimas Gumerang Ryandika,Setyawan Suroso dan Indra Agrisetya selaku sahabat yang telah mendukung dan membantu penulis selama menempuh dan menyelesaikan masa studi di Institut Teknologi Telkom Purwokerto.
11. Zen Firman dan Muhamad Junaidi selaku teman dari SMK yang telah mendukung dan membantu penulis selama menempuh dan menyelesaikan masa studi di Institut Teknologi Telkom Purwokerto.
12. 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,7 Agustus 2023

Penulis



(Aziz Tri Nugroho)

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.
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.
Merkle-hellman Knapsack	: Methode kriptografi asimetris dengan perhitungan invers dan modulus.

DAFTAR SINGKATAN

BSSN	: Badan Siber dan Sandi Negara
CPU	: Central Processing Unit
RP	: Rupiah
SQL	: Structured query language
CSS	: Cascading Style sheets
HTML	: HyperText Markup Language
AES	: Advanced Encryption Standard
DES	: Data Encyprion Standard
RAM	: Random Access Memory
HDD	: Hard Disk Drive
SSD	: Solid State Drive
SSL	: Secure Socket Layer
JS	: Java Script
PHP	: Hypertext Preprocessor