



LAPORAN SKRIPSI

**PENERAPAN ALGORITMA AES UNTUK KEAMANAN
FILE (STUDI KASUS : PENDAFTARAN TANAH
SISTEMATIS LENGKAP (PTSL) DI DESA
KEDUNGSARI)**

**ADHIN NAFA RIZAL FIKRI
NIM. 201951254**

**DOSEN PEMBIMBING
Ratih Nindyasari, S.Kom, M.Kom
Alif Catur Murti, S.Kom, M.Kom**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MURIA KUDUS
AGUSTUS 2023**

HALAMAN PERSETUJUAN

**PENERAPAN ALGORITMA AES UNTUK KEAMANAN *FILE*
(STUDI KASUS : PENDAFTARAN TANAH SISTEMATIS
LENGKAP (PTSL) DI DESA KEDUNGSARI)**

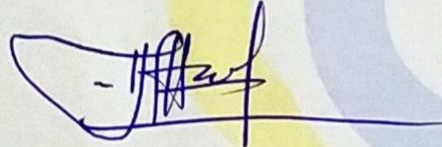
ADHIN NAFA RIZAL FIKRI

NIM. 201951254

Kudus, 21 Juli 2023

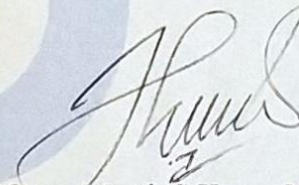
Menyetujui,

Pembimbing Utama,



**Ratih Nindyasari, S.Kom., M.Kom.
NIDN. 0625028501**

Pembimbing Pendamping,



**Alif Catur Murti, S.Kom., M.Kom.
NIDN. 0610129001**

HALAMAN PENGESAHAN

**PENERAPAN ALGORITMA AES UNTUK KEAMANAN *FILE*
(STUDI KASUS : PENDAFTARAN TANAH SISTEMATIS
LENGKAP (PTSL) DI DESA KEDUNGSARI)**

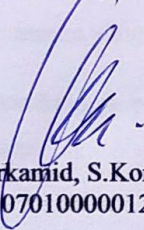
ADHIN NAFA RIZAL FIKRI

NIM. 201951254

Kudus, 12 Agustus 2023

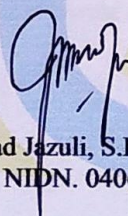
Menyetujui,

Ketua Penguji,



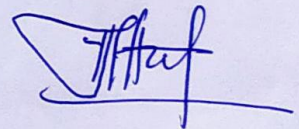
**Mukhamad Nurkamid, S.Kom., M.Cs.
NIS. 0610701000001212**

Anggota Penguji I,



**Ahmad Jazuli, S.Kom., M.Kom.
NIDN. 0406107004**

Anggota Penguji II,



**Ratih Nindyasari, S.Kom., M.Kom.
NIDN. 0625028501**

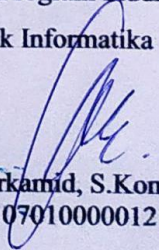
Mengetahui

Dekan Fakultas Teknik



**Mohammad Dahlan, S.T., M.T.
NIS. 0610701000001141**

**Ketua Program Studi
Teknik Informatika**



**Mukhamad Nurkamid, S.Kom., M.Cs.
NIS. 0610701000001212**

PERNYATAAN KEASLIAN

Saya yang bertanda tangan dibawah ini :

Nama : Adhin Nafa Rizal Fikri
NIM : 201951254
Tempat & Tanggal Lahir : Kudus, 14 November 2001
Judul Skripsi : Penerapan Algoritma AES Untuk Keamanan *File*
(Studi Kasus : Pendaftaran Tanah Sistematis
Lengkap (PTSL) Di Desa Kedungsari)

Menyatakan dengan sebenarnya bahwa penulisan Skripsi ini berdasarkan hasil penelitian, pemikiran dan pemaparan asli dari saya sendiri, baik untuk naskah laporan maupun kegiatan lain yang tercantum sebagai bagian dari Skripsi ini. Seluruh ide, pendapat, atau materi dari sumber lain telah dikutip dalam Skripsi dengan cara penulisan referensi yang sesuai.

Demikian pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar dan sanksi lain sesuai dengan peraturan yang berlaku di Universitas Muria Kudus.

Demikian pernyataan ini saya buat dalam keadaan sadar tanpa paksaan dari pihak manapun.

Kudus, 12 Agustus 2023

Yang memberi pernyataan,



Adhin Nafa Rizal Fikri
NIM. 201951254

KATA PENGANTAR

Puji syukur kehadiran Allah SWT karena atas Rahmat dan Hidayah-Nya penulis mampu menyelesaikan penyusunan skripsi ini dengan judul “Penerapan Algoritma AES Untuk Keamanan *File* (Studi Kasus : Pendaftaran Tanah Sistematis Lengkap (PTSL) Di Desa Kedungsari)”. Skripsi ini disusun guna melengkapi salah satu persyaratan untuk menyelesaikan jenjang pendidikan Strata Satu (S1) pada Program Studi Teknik Informatika Fakultas Teknik Universitas Muria Kudus. Pada kesempatan ini, penulis ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada :

1. Allah SWT yang telah memberikan Rahmat dan Hidayah-Nya.
2. Bapak Mukhamad Nurkamid, S.Kom., M.Cs., selaku Ketua Program Studi Teknik Informatika Universitas Muria Kudus.
3. Ibu Ratih Nindyasari, S.Kom., M.Kom., selaku pembimbing I yang telah banyak memberikan masukan selama penyusunan skripsi ini.
4. Bapak Alif Catur Murti, S.Kom., M.Kom., selaku pembimbing II yang telah banyak memberikan masukan selama penyusunan skripsi ini.
5. Kedua orang tua, Bapak dan Ibu yang selalu memberi semangat dan do'a kepada penulis.
6. Teman-teman angkatan 2019 Program Studi Teknik Informatika Universitas Muria Kudus yang selalu memberikan semangat dan dukungan satu sama lain.

Penulis menyadari sepenuhnya bahwa dalam penyusunan skripsi ini masih terdapat banyak kekurangan. Selain itu penulis juga berharap semoga karya tulis ini dapat memberikan manfaat bagi semua.

Kudus, 12 Agustus 2023

Penulis

PENERAPAN ALGORITMA AES UNTUK KEAMANAN *FILE* (STUDI KASUS : PENDAFTARAN TANAH SISTEMATIS LENGKAP (PTSL) DI DESA KEDUNGSARI)

Nama mahasiswa : Adhin Nafa Rizal Fikri

NIM : 201951254

Pembimbing :

1. Ratih Nindyasari, S.Kom., M.Kom.
2. Alif Catur Murti, S.Kom., M.Kom.

RINGKASAN

Teknologi sekarang ini semakin berkembang seiring dengan meningkatnya kebutuhan manusia tentang informasi. Informasi tersebut dapat didapatkan secara mudah dari berbagai macam sumber. Dari berbagai macam informasi tersebut, terdapat informasi yang harus dilindungi dan dijaga keamanannya. Salah satu contohnya adalah *file* data Pendaftaran Tanah Sistematis Lengkap (PTSL) di Desa Kedungsari, Kecamatan Gebog, Kabupaten Kudus yang berisikan data pertanahan dari para pendaftar PTSL. Data tersebut bersifat vital dan sangat berpotensi untuk disalahgunakan oleh orang yang tidak bertanggung jawab. Untuk menghindari hal tersebut dapat digunakan suatu metode yaitu kriptografi. Salah satu algoritma kriptografi yaitu algoritma *Advanced Encryption Standard (AES) 128 bit* yang merupakan penyempurnaan dari algoritma *DES*. Diharapkan algoritma *Advanced Encryption Standard (AES) 128 bit* dapat digunakan sebagai sarana pengamanan data Pendaftaran Tanah Sistematis Lengkap (PTSL) di Desa Kedungsari dari akses pihak yang tidak berkepentingan dengan tahap pengujian terdiri dari 2 tahapan yaitu pengujian validitas dan pengujian performa.

Kata kunci : *AES*, *PTSL*, *file*.

**APPLICATION OF AES ALGORITHM FOR FILE SECURITY (CASE
STUDY: COMPLETE SYSTEMATIC LAND REGISTRATION (PTSL) IN
KEDUNGSARI VILLAGE)**

Student Name : Adhin Nafa Rizal Fikri

Student Identity Number : 201951254

Supervisor :

1. Ratih Nindyasari, S.Kom, M.Kom

2. Alif Catur Murti, S.Kom, M.Kom

ABSTRACT

Today's technology is growing along with the increasing human need for information. This information can be obtained easily from various sources. Of the various kinds of information, there is information that must be protected and safeguarded. One example is the Complete Systematic Land Registration (PTSL) data file in Kedungsari Village, Gebog District, Kudus Regency which contains land data from PTSL applicants. This data is vital and has the potential to be misused by irresponsible people. To avoid this can be used a method that is cryptography. One of the cryptographic algorithms is the 128-bit Advanced Encryption Standard (AES) algorithm which is a refinement of the DES algorithm. It is hoped that the 128-bit Advanced Encryption Standard (AES) algorithm can be used as a means of securing Complete Systematic Land Registration (PTSL) data in Kedungsari Village from access by unauthorized parties. The testing phase consists of 2 stages, namely validity testing and performance testing.

Keywords : AES,PTSL,file

DAFTAR ISI

HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
PERNYATAAN KEASLIAN.....	iv
KATA PENGANTAR	v
RINGKASAN	vi
<i>ABSTRACT</i>	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
DAFTAR LAMPIRAN.....	xii
DAFTAR ISTILAH DAN SINGKATAN	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah.....	2
1.3. Batasan Masalah.....	2
1.4. Tujuan.....	2
1.5. Sistematika penulisan	2
1.5.1. BAB I Pendahuluan	3
1.5.2. BAB II Tinjauan Pustaka	3
1.5.3. BAB III Metodologi.....	3
1.5.4. BAB IV Hasil Dan Pembahasan	3
1.5.5. BAB V Penutup	3
1.6. Alat yang digunakan.....	3
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Sebelumnya	5
2.2. Landasan Teori	8
2.2.1. Pendaftaran Tanah Sistematis Lengkap (PTSL)	8
2.2.2. Kriptografi.....	8
2.2.3. <i>Advanced Encryption Standard</i> (AES)	8
2.2.4. <i>Data Flow Diagram</i> (DFD)	12
2.2.5. <i>Entity Relationship Diagram</i> (ERD)	13
2.2.6. <i>Flowchart</i>	14

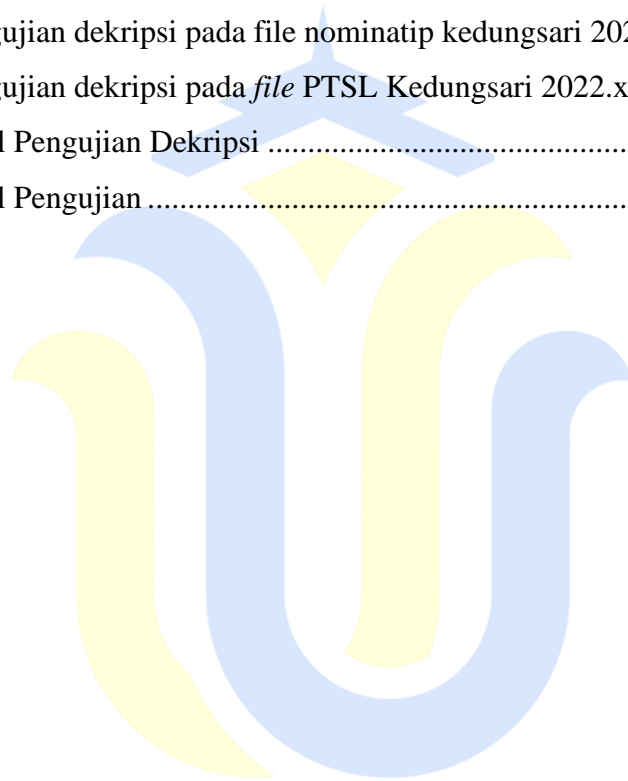
2.2.7. Pengembangan Sistem Prototype.....	14
BAB III METODOLOGI.....	17
3.1. Metode Pengumpulan Data	17
3.2. Metode Pengembangan Sistem <i>Prototype</i>	17
3.3. Enkripsi <i>Advanced Encryption Standard (AES)</i> 128 bit.....	17
3.4. Dekripsi <i>Advanced Encryption Standard (AES)</i> 128 bit.....	35
BAB IV HASIL DAN PEMBAHASAN	49
4.1. Perancangan Sistem.....	49
4.1.1. <i>Flowchart</i>	49
4.1.2. <i>Entity Relationship Diagram (ERD)</i>	50
4.1.3. <i>Data Flow Diagram (DFD)</i>	50
4.1.4. <i>Desain Interface</i>	52
4.2. Penerapan Pada Aplikasi	53
4.3. Proses Enkripsi Dekripsi File dengan AES-128.....	56
4.3.1. Enkripsi File	56
4.3.2. Dekripsi File.....	62
4.4. Pengujian Validitas Algoritma	66
4.5. Pengujian Performa	67
4.5.1. Enkripsi	67
4.5.2. Dekripsi.....	69
4.5.3. Hasil Pengujian Performa	70
BAB V PENUTUP.....	71
5.1. Kesimpulan.....	71
5.2. Saran.....	71
DAFTAR PUSTAKA	72
LAMPIRAN 1	73
LAMPIRAN 2	77
LAMPIRAN 3.....	78
LAMPIRAN 4.....	81
LAMPIRAN 5.....	82
LAMPIRAN 6.....	83
LAMPIRAN 7.....	84
LAMPIRAN 8.....	85
LAMPIRAN 9.....	86
BIODATA PENULIS	87

DAFTAR GAMBAR

Gambar 2. 1 Proses Enkripsi AES	9
Gambar 2. 2 AES SBOX.....	10
Gambar 2. 3 Proses Dekripsi AES	11
Gambar 2. 4 InvSBox.....	12
Gambar 2. 5. <i>Flowchart</i>	14
Gambar 2. 6. Pengembangan prototype	15
Gambar 3. 1. Proses Enkripsi AES-128.....	18
Gambar 3. 2 AES SBOX.....	19
Gambar 3. 3 Operasi <i>SubByte</i>	23
Gambar 3. 4. Proses Dekripsi AES-128.....	35
Gambar 3. 5 InvSBOX.....	36
Gambar 4. 1. Flowchart Program.....	49
Gambar 4. 2. ERD Sistem.....	50
Gambar 4. 3. DFD <i>level 0</i>	51
Gambar 4. 4. DFD <i>level 1</i>	51
Gambar 4. 5. Interface Login	52
Gambar 4. 6. Interface Dashboard	52
Gambar 4. 7. Interface halaman keseluruhan.....	53
Gambar 4. 8. Halaman <i>Login</i>	53
Gambar 4. 9. Halaman <i>Dashboard</i>	54
Gambar 4. 10 tampilan daftar <i>file</i> terenkripsi dan terdekripsi	54
Gambar 4. 11 Tampilan tambah <i>file</i> enkripsi.....	54
Gambar 4. 12 Tabel File terenkripsi dan Terdekripsi	55
Gambar 4. 13 Tampilan dekripsi file	55
Gambar 4. 14 Halaman daftar <i>file</i> siap <i>download</i>	56
Gambar 4. 15 Plaintext file	66
Gambar 4. 16 Ciphertext file.....	67

DAFTAR TABEL

Tabel 2. 1. Perbandingan jurnal sebelumnya	6
Tabel 2. 2. DFD.....	12
Tabel 2. 3. ERD.....	13
Tabel 3. 1. Tabel RCON	18
Tabel 4. 1. Pengujian enkripsi pada <i>file</i> nominatip kedungsari 2021.xlsx.....	67
Tabel 4. 2. Pengujian enkripsi pada <i>file</i> PTSL Kedungsari 2022.xlsx.....	68
Tabel 4. 3 Hasil pengujian Enkripsi.....	68
Tabel 4. 4. Pengujian dekripsi pada file nominatip kedungsari 2021.xlsx	69
Tabel 4. 5. Pengujian dekripsi pada <i>file</i> PTSL Kedungsari 2022.xlsx.....	69
Tabel 4. 6. Hasil Pengujian Dekripsi	70
Tabel 4. 7. Hasil Pengujian	70



DAFTAR LAMPIRAN

- Lampiran 1. Lampiran Bimbingan
- Lampiran 2. Hasil Turnitin
- Lampiran 3. Lampiran Revisi Sidang
- Lampiran 4. Surat Balasan Izin Penelitian
- Lampiran 5. Instrumen Penelitian
- Lampiran 6. Artikel Ilmiah
- Lampiran 7. Poster
- Lampiran 8. *Manual Book*
- Lampiran 9. Dokumentasi
- Lampiran 10. Biodata Diri



DAFTAR ISTILAH DAN SINGKATAN

PTSL	: Pendaftaran Tanah Sistematis Lengkap
AES	: <i>Advanced Encryption Standard</i>
XOR	: <i>Exclusive Or</i>
DFD	: <i>Data Flow Diagram</i>
ERD	: <i>Entity Relationship Diagram</i>

