



## BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR

S/UBL/FTI/0674/II/26

Pada hari ini, Senin 09 Februari 2026 telah dilaksanakan Ujian Sidang Pendadaran Tugas Akhir sebagai berikut:

Judul: IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA FILE MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) DENGAN KEY EXPANSION

Nama : Indika In Amuloh  
NIM : 1911511721  
Dosen Pembimbing : Purwanto, S.Si, M.Kom.

Berdasarkan penilaian pada Presentasi + Demo, Penulisan, Penguasaan Materi, Penguasaan Program maka Mahasiswa tersebut di atas dinyatakan:

**LULUS**

dengan nilai angka : **80** huruf : **A-**

Mahasiswa tersebut di atas wajib menyerahkan hasil perbaikan tulisan Tugas Akhir dalam bentuk terjilid sesuai dengan Panduan Perbaikan Tugas Akhir, selambat-lambatnya Senin 23 Februari 2026.

### Panitia Penguji:

- 1 Ketua Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom.
- 2 Anggota Sejati Waluyo, S.Kom., M.Kom.
- 3 Moderator Purwanto, S.Si, M.Kom.

### Keterangan:

Nilai Huruf: A:85-100 A-:80-84,99 B+:75-79,99 B:70-74,99 B-:65-69,99 C:60-64,99 D:40-59,99 E-:0-39,99



UNIVERSITAS BUDI LUHUR  
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 1911511721

Nama: Indika In Amuloh

Pembimbing: Purwanto, S.Si, M.Kom.

No.	Tanggal	Materi
1	11-10-2025	Konsultasi dan Pengajuan Topik/Judul
2	17-10-2025	Penyerahan BAB 1
3	25-10-2025	Revisi dan Konsultasi BAB 1
4	08-11-2025	Penyerahan BAB 2
5	14-11-2025	Revisi dan Konsultasi BAB 2
6	29-11-2025	Penyerahan BAB 3
7	05-12-2025	Revisi dan Konsultasi BAB 3
8	15-12-2025	Demo Program
9	05-01-2026	Penyerahan dan Konsultasi BAB 4
10	09-01-2026	Revisi dan Konsultasi BAB 4 & Penyerahan BAB 5
11	19-01-2026	Revisi BAB 5 & Demo Program



LEMBAR PENGESAHAN

Nama : Indika In Amuloh  
Nomor Induk Mahasiswa : 1911511721  
Program Studi : Teknik Informatika  
Bidang Peminatan : Programming Expert  
Jenjang Studi : Strata 1  
Judul : IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA FILE  
MENGUNAKAN ALGORITMA ADVANCED ENCRYPTION  
STANDARD (AES) DENGAN KEY EXPANSION



Laporan Tugas Akhir ini telah disetujui, disahkan dan direkam secara elektronik sehingga tidak memerlukan tanda tangan tim penguji.

Jakarta, Senin 09 Februari 2026

Tim Penguji:

Ketua : Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom.  
Anggota : Sejati Waluyo, S.Kom., M.Kom.  
Pembimbing : Purwanto, S.Si, M.Kom.  
Ketua Program Studi : Dr. Indra, S.Kom., M.T.I.

## DAFTAR TABEL

Tabel 2.1 Parameter <i>AES</i> .....	11
Tabel 2.2. Studi Literatur .....	17
Tabel 3.1 Metode Pembanding .....	30
Tabel 3.2 Tabel <i>User</i> .....	36
Tabel 3.3 <i>file_record</i> .....	37
Tabel 3.4 Alur Penggunaan Sistem.....	38
Tabel 4.1 Pengujian Enkripsi Dekripsi .....	57
Tabel 4.2 Hasil Pengujian Waktu Enkripsi dan Dekripsi per <i>File</i> .....	58

## DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Proses Enkripsi <i>AES</i> .....	12
Gambar 2.2 Ilustrasi Proses Dekripsi <i>AES</i> .....	13
Gambar 3.1 Class Diagram.....	36
Gambar 3.2 Rancangan Menu .....	38
Gambar 4.1 <i>Deployment Diagram</i> .....	41
Gambar 4.2 Alur Proses <i>Key Expansion</i> .....	42
Gambar 4.3 Alur Algoritma <i>AES</i> .....	43
Gambar 4.4 Alur API dan <i>Database</i> .....	45
Gambar 4.5 <i>Flowchart</i> Enkripsi .....	46
Gambar 4.6 <i>Flowchart</i> Dekripsi .....	47
Gambar 4.7 <i>Flowchart</i> alur program .....	48
Gambar 4.8 S-Box SubBytes .....	50
Gambar 4.9 Pengaruh Pemetaan pada Setiap <i>Byte</i> dalam State .....	51
Gambar 4.10 Transformasi <i>ShiftRows</i> .....	51
Gambar 4.11 Transformasi <i>InvShiftRows</i> .....	52
Gambar 4.12 Tabel Inverse S-Box. ....	53
Gambar 4.13 Proses Representasi Matematis Transformasi <i>Key Expansion</i> <i>AES-128</i> .....	54
Gambar 4.14 Form Login .....	60
Gambar 4.15 <i>Dashboard</i> - Total dan Aktifitas Diagram .....	61
Gambar 4.16 <i>Dashboard</i> - Rasio dan <i>File</i> Terbaru.....	61
Gambar 4.17 Tampilan Halaman <i>Profile</i> .....	62
Gambar 4.18 Tampilan Halaman Enkripsi .....	63
Gambar 4.19 Tampilan Halaman Dekripsi .....	64

## DAFTAR SIMBOL

Simbol 4.1 Transformasi Mix Column Rinci .....	51
Simbol 4.2 Transformasi Mix Column Setara .....	52
Simbol 4.3 Transformasi <i>InvMixColumn</i> Tahap Enkripsi .....	53
Simbol 4.3 Transformasi <i>InvMixColumn</i> Bentuk Persamaan.....	54

## DAFTAR MODUL

Modul 4.1 <i>Source Code</i> Modifikasi <i>S-Box</i> .....	55
Modul 4.2 <i>Source Code</i> Modifikasi Round Constant.....	55

## DAFTAR ISI

<b>COVER DEPAN</b> .....	<b>i</b>
<b>COVER DALAM</b> .....	<b>ii</b>
<b>LEMBAR PENGESAHAN</b> .....	<b>iii</b>
<b>ABSTRAK</b> .....	<b>iv</b>
<b>ABSTRACT</b> .....	<b>v</b>
<b>SURAT PERNYATAAN TIDAK PLAGIAT DAN PERSETUJUAN PUBLIKASI</b> .....	<b>vi</b>
<b>KATA PENGANTAR</b> .....	<b>viii</b>
<b>DAFTAR TABEL</b> .....	<b>x</b>
<b>DAFTAR GAMBAR</b> .....	<b>xi</b>
<b>DAFTAR SIMBOL</b> .....	<b>xii</b>
<b>DAFTAR MODUL</b> .....	<b>xiii</b>
<b>DAFTAR ISI</b> .....	<b>xiv</b>
<b>Bab I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang .....	1
1.2 Perumusan Masalah .....	2
1.3 Batasan Masalah .....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
1.6 Sistematika Penulisan .....	5
<b>Bab II LANDASAN TEORI</b> .....	<b>7</b>
2.1 Kriptografi .....	7
2.2 Algoritma <i>AES</i> .....	9
2.3 <i>Key Expansion</i> .....	13
2.4 Modifikasi <i>Key Expansion</i> .....	14
2.5 Pengamanan Data File .....	14

2.6 <i>Python</i> .....	16
2.7 Studi Literatur .....	17
<b>Bab III METODOLOGI PENELITIAN .....</b>	<b>29</b>
3.1 Data Penelitian .....	29
3.2 Metode Perbandingan .....	30
3.3 Metode Penelitian .....	32
3.4 Rancangan Pengujian.....	34
3.5 Rancangan Basis Data .....	35
3.6 Rancangan Menu .....	37
3.7 Rancangan Layar .....	38
<b>Bab IV HASIL DAN PEMBAHASAN.....</b>	<b>40</b>
4.1 Analisis <i>Input</i> .....	40
4.2 Analisis <i>Output</i> .....	41
4.3 <i>Flowchart</i> .....	46
4.4 Algoritma .....	49
4.5 Pengujian.....	56
4.6 Tampilan Layar Aplikasi.....	59
<b>Bab V PENUTUP .....</b>	<b>65</b>
5.1 Kesimpulan .....	65
5.2 Saran .....	66
<b>DAFTAR PUSTAKA.....</b>	<b>67</b>
<b>LAMPIRAN-LAMPIRAN .....</b>	<b>70</b>