



UNIVERSITAS BUDI LUHUR  
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 2111510323

Nama: Muhamad Ilham Hasmardian

Pembimbing: Joko Christian Chandra, S.Kom., M.Kom.

No.	Tanggal	Materi
1	06-10-2025	Draft bab 1
2	18-10-2025	perbaikan bab 1 + draft bab 2
3	02-11-2025	perbaikan bab 2 + draft bab 3
4	02-12-2025	Demo aplikasi + flowchart + draft bab 4
5	19-12-2025	bab 4 + demo aplikasi
6	07-01-2026	bab 5 + perbaikan bab 4
7	14-01-2026	Keseluruhan bab versi alfa
8	22-02-2026	perbaikan bab 3 + draft bab 4



## BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR

S/UBL/FTI/0543/II/26

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

Judul: IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) COUNTER MODE DENGAN PEMBANGKITAN INITIAL VECTOR BERBASIS METADATA FILE UNTUK PENGAMANAN ASET DIGITAL PADA PT QUANTUM TERA NETWORK

Nama : Muhamad Ilham Hasmardian  
NIM : 2111510323  
Dosen Pembimbing : Joko Christian Chandra, S.Kom., M.Kom.

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

**LULUS**

dengan nilai angka : **75** huruf : **B+**

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 Haris Munandar, S.T, M.T.I.
- 2 Anggota Dr. Mohammad Syafrullah, M.Kom, M.Sc.
- 3 Moderator Joko Christian Chandra, S.Kom., 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



**IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDARD  
(AES-128) COUNTER MODE DENGAN MODIFIKASI PEMBANGKITAN  
INITIAL VECTOR BERBASIS METADATA FILE UNTUK  
PENGAMANAN ASET DIGITAL PADA PT QUANTUM TERA  
NETWORK.  
LAPORAN TUGAS AKHIR**

**Oleh:**

**NIM  
1. 2111510323**

**NAMA  
Muhamad Ilham Hasmardian**

**FAKULTAS TEKNOLOGI INFORMASI  
UNIVERSITAS BUDI LUHUR**

**JAKARTA  
SEMESTER GASAL  
2025/2026**

## ABSTRAK

PT Quantum Tera Network merupakan perusahaan *Internet Service Provider* (ISP) yang mengelola aset digital sensitif pada divisi *Network Operation Center* (NOC), seperti daftar *IP Public*, register klien, dan Surat Perintah Kerja (SPK). Saat ini, aset tersebut masih disimpan dalam format berkas asli (*plaintext*) yang rentan terhadap risiko akses ilegal dan kebocoran data. Penelitian ini bertujuan untuk merancang sistem pengamanan berkas menggunakan algoritma kriptografi simetris \$AES-128\$ dengan mode operasi *Counter* (CTR). Inovasi utama dalam penelitian ini terletak pada modifikasi mekanisme pembangkitan *Initial Vector* (IV) yang diekstraksi secara dinamis dari metadata berkas, meliputi nama berkas, ukuran, dan waktu modifikasi dalam skala nanodetik. Hal ini dilakukan untuk menjamin keunikan *keystream* dan mencegah risiko *nonce reuse* pada mode CTR. Sistem dikembangkan menggunakan bahasa pemrograman Python dengan *framework* Flask dan basis data MySQL. Hasil pengujian menunjukkan bahwa aplikasi mampu menjaga integritas berkas secara utuh dan memiliki efisiensi performa yang sangat tinggi, di mana proses enkripsi dan dekripsi untuk berkas berukuran hingga 25 MB dapat diselesaikan dalam waktu kurang dari 0,1 detik. Implementasi ini memberikan solusi pengamanan aset digital yang tangguh namun tetap menjaga produktivitas operasional pada PT Quantum Tera Network.

**Kata Kunci:** *Kriptografi, \$AES-128\$, Counter Mode, Initial Vector, Metadata Berkas, PT Quantum Tera Network.*

10+59 halaman, 17 gambar, 9 tabel, 2 lampiran

## DAFTAR ISI

COVER.....	i
ABSTRAK.....	ii
SURAT PERNYATAAN TIDAK PLAGIAT .....	iii
KATA PENGANTAR .....	iv
DAFTAR TABEL .....	v
DAFTAR GAMBAR .....	vi
DAFTAR SIMBOL.....	vii
DAFTAR ISI.....	ix
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Identifikasi Masalah .....	2
1.3. Perumusan Masalah .....	2
1.4. Batasan Masalah .....	3
1.5. Tujuan Penelitian .....	3
1.6. Manfaat Penelitian.. .....	4
1.6. Sistematika Penulisan .....	4
BAB II LANDASAN TEORI.....	6
2.1. Tinjauan Studi.....	6
2.1.1. Implementasi pada Lingkungan Instansi dan Korporasi.. .....	6
2.2. Konsep Dasar Kriptografi.....	6
2.2.1. Algoritma Advanced Encryption Standard (AES).. .....	7
2.2.2. Mode Operasi Counter (CTR).. .....	9
2.3. Initial Vector (IV) dan Masalah <i>Nonce Reuse</i> .....	9
2.4. Metadata File Sistem .....	10
2.5. Pengujian... .....	10
2.5.1. Black Box Testing.....	11
2.5.2. White Box Testing.. .....	11
2.6. Studi Literatur... .....	11
2.6.1. Perbandingan... .....	14
2.7. Kerangka Pemikiran... .....	15
BAB III METODOLOGI PENELITIAN .....	17
3.1. Data Penelitian .....	17
3.1.1. Objek Penelitian.....	17
3.1.2. Sumber Data .....	18
3.2. Metode Pembanding .....	19
3.2.1. Posisi Penelitian .....	19
3.2.2. Analisis Penelitian.....	20
3.2.3. Kontribusi dan Posisi Penelitian .....	21
3.3. Metode Penelitian .....	22
3.3.1. Tahap Analisi Kebutuhan Sistem .....	22
3.3.2. Tahap Perancangan Sistem .....	23
3.3.3. Tahap Perancangan dan Implementasi Algoritma Kriptografi ..	24
3.4. Rancangan Pengujian.....	26
3.4.1. Pengujian Fungsional.....	26

3.4.2. Pengujian Performa.....	27
3.5. Rancangan Basis Data .....	28
3.6. Rancangan Menu .....	29
3.7. Rancangan Layar .....	31
3.7.1.Rancangan Layar Login.....	31
3.7.2.Rancangan Layar Dashboard .....	31
3.7.3.Rancangan Layar Enkripsi File.....	32
3.7.4.Rancangan Layar Dekripsi.....	33
BAB IV HASIL DAN PEMBAHASAN .....	34
4.1. Lingkungan Percobaan .....	34
4.1.1. Spesifikasi Hardware .....	34
4.1.2. Spesifikasi Software .....	35
4.1.3. Arsitektur Deployment.....	35
4.2. Implementasi Metode .....	36
4.2.1. Tahapan Pengolahan Kunci ( <i>Key Handling</i> ).....	37
4.2.2. Tahapan Pembangkitan IV Berbasis Metadata (Modifikasi) .....	38
4.2.3. Tahapan Enkripsi AES-CTR secara <i>Scratch</i> .....	39
4.2.4. Tahapan Proses Dekripsi File.....	40
4.2.5. Integrasi Metode dengan Sistem Aplikasi .....	40
4.3. FlowChart .....	40
4.3.1. Flowchart Keseluruhan .....	41
4.3.2. Flowchart Metode Logika AES-128 CTR .....	42
4.3.3. Flowchart Proses Enkripsi File .....	43
4.3.4. Flowchart Proses Dekripsi File.....	44
4.4. Implementasi Algoritma .....	46
4.4.1. Algoritma Enkripsi File AES-128 CTR ( <i>Scratch</i> ).....	47
4.4.2. Algoritma Pembangkitan Initial Vector (IV) Berbasis Metadata File .....	49
4.5. Pengujian Sistem.....	50
4.5.1. Skenario Pengujian .....	50
4.5.2. Hasil Pengujian .....	51
4.6. Analisa Hasil Pengujian .....	51
4.6.1. Analisis Efisiensi Waktu Proses .....	51
4.6.2. Analisis Efisiensi Waktu Proses .....	52
4.6.3. Analisis Keunikan Initial Vector (IV) Berbasis Metadata .....	52
4.7. Tampilan Layar Aplikasi.....	53
4.7.1. Halaman Login .....	53
4.7.2. Tampilan Halaman Dashboard.....	54
4.7.3. Tampilan Halaman Enkripsi File.....	54
4.7.4. Tampilan Halaman Dekripsi .....	56
4.7.5. Tampilan Halaman History. ....	57
BAB V PENUTUP .....	58
5.1 Kesimpulan .....	58
5.2 saran .....	58
DAFTAR PUSTAKA.....	60
LAMPIRAN.....	61

## DAFTAR PUSTAKA

- Aprizaldi, Hasan, M. A., & Setiawan, D. (2023). Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data. *Jurnal Teknik Informatika*, 2(2).
- Aryanto, M. B., Tahir, M., Devita, S. I., Mustofa, Z. N., Ainiyah, Q., & Sundoro, S. (2023). Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128). *JUISIK (Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer)*, 3(1), 89-104.
- Fahlevvi, M. R., Putra, D. S. A., & Ariandi, W. (2025). ALGORITMA AES128-CBC (ADVANCED ENCRYPTION STANDARD) UNTUK ENKRIPSI DAN DEKRIPSI BERKAS DOKUMEN PT. ADIARTA MUZIZAT. *Jurnal Innovation and Future Technology (IFTECH)*, 7(1).
- Hidayatuloh, F., Amila, Y., Akbar, M. N. N., Maesaroh, S., & Firmansyah, F. (2026). Komparasi Performa dan Keamanan Algoritma AES-128 dan Blowfish pada Enkripsi Berkas Teks. *Jejakdigital: Jurnal Ilmiah Multidisiplin*, 2(1), 1674-1677.
- Sagala, H. A. (2023). Perancangan Aplikasi Audit Internal Dengan Menerapkan Algoritma AES 128 Bit Untuk Pengamanan Data. *Journal Global Technology Computer*, 2(2), 75-86.
- Sijabat, N., Hayaty, N., & Suswaini, E. (2022). IMPLEMENTASI KRIPTOGRAFI HYBRID MENGGUNAKAN ALGORITMA AES-128 DAN ALGORITMA RABIN UNTUK MENGAMANKAN DATA DALAM DATABASE. *Student Online Journal (SOJ)*, 3(1).
- Suranta, A. I., & Sakti, D. V. S. Y. (2022). Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 5(1), 1-10.
- Tania, M., Alasi, T. S., & Yap, R. (2024). ALGORITMA AES UNTUK KEAMANAN DATA DIGITAL BERBASIS WEB DI KANTOR DESA AMAN DAMAI. *Jurnal TIMES*, 13(2).
- Tarigan, Y. A. P., Aulia, R., & Elhanafi, A. M. (2024). Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web. *Jurnal Unitek*, 17(2), 196-203.
- Widyawan, D., & Imelda. (2021). PENGAMANAN FILE MENGGUNAKAN KRIPTOGRAFI DENGAN METODE AES-128 BERBASIS WEB DI KOMITE NASIONAL KESELAMATAN TRANSPORTASI. *SKANIKA: Sistem Komputer dan Teknik Informatika*, 4(1), 15-22.