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

UNIVERSITAS BUDI LUHUR
Kampus Pusat : Jl. Raya Ciledug - Petukangan Utara - Jakarta Selatan 12260
Telp : 021-5853753 (hunting), Fax : 021-5853489, http://www.budiluhur.ac.id
FAKULTAS TEKNOLOGI INFORMASI
FAKULTAS EKONOMI DAN BISNIS
FAKULTAS ILMU SOSIAL DAN STUDI GLOBAL
FAKULTAS TEKNIK
FAKULTAS KOMUNIKASI DAN DESAIN KREATIF

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	NAMA
1. 2111510323	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

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.