



UNIVERSITAS BUDI LUHUR
FAKULTAS TEKNOLOGI INFORMASI

Kartu Bimbingan Tugas Akhir

NIM: 2111510596

Nama: Risqi Rahman Pratama

Pembimbing: Dolly Virgiana Shaka Yudha Sakti, S.Kom., M.Kom.

No.	Tanggal	Materi
1	14-04-2025	pembahasan perkembangan skripsi 1 (aplikasi web chatting dengan enkripsi)
2	23-04-2025	pembahasan penggunaan algoritma asimetris pada chatting
3	23-05-2025	Menggunakan Aes 256 dan ECC pada pedan teks dan file dan shared hosting
4	17-06-2025	pembahasan bab 1 dan 2 skripsi
5	20-06-2025	pembahasan bab 3 rancangan database
6	24-06-2025	rancangan menu , deployment diagram, dan flowchart
7	26-06-2025	proses rancangan layar dan keterangan riset
8	08-07-2025	Penyelsaian skripsi
9	08-07-2025	Penyelsaian skripsi



BERITA ACARA SIDANG PENDADARAN TUGAS AKHIR

S/UBL/FTI/0812/VII/25

Pada hari ini, Senin 14 Juli 2025 telah dilaksanakan Ujian Sidang Pendadaran Tugas Akhir sebagai berikut:

Judul: APLIKASI CHATTING DAN FILE SHARING BERBASIS WEB MENGGUNAKAN HYBRID ENCRYPTION AES 256 GCM DAN ECC X25519 PADA SHARED HOSTING PT APRILIA TEKNOLOGI MANDIRI

Nama : Risqi Rahman Pratama
NIM : 2111510596
Dosen Pembimbing : Dolly Virgian Shaka Yudha Sakti, S.Kom., M.Kom.

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

LULUS

dengan nilai angka : **85** 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 28 Juli 2025.

Panitia Penguji:

- | | |
|-------------|---|
| 1 Ketua | Gunawan Pria Utama, S.Kom., M.Kom. |
| 2 Anggota | Krisna Adiyarta Musodo, Ph.D. |
| 3 Moderator | Dolly Virgian Shaka Yudha Sakti, 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



LEMBAR PENGESAHAN

Nama	: Risqi Rahman Pratama
Nomor Induk Mahasiswa	: 2111510596
Program Studi	: Teknik Informatika
Bidang Peminatan	: Programming Expert
Jenjang Studi	: Strata 1
Judul	: APLIKASI CHATting DAN FILE SHARING BERBASIS WEB MENGUNAKAN HYBRID ENCRYPTION AES 256 GCM DAN ECC X25519 PADA SHARED HOSTING PT APRILIA TEKNOLOGI MANDIRI



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

Jakarta, Senin 14 Juli 2025

Tim Penguji:

Ketua	: Gunawan Pria Utama, S.Kom., M.Kom.
Anggota	: Krisna Adiyarta Musodo, Ph.D.
Pembimbing	: Dolly Virgiana Shaka Yudha Sakti, S.Kom., M.Kom.
Ketua Program Studi	: Dr. Indra, S.Kom., M.T.I.

**APLIKASI CHATting DAN FILE SHARING BERBASIS WEB
MENGUNAKAN HYBRID ENCRYPTION AES 256 GCM
DAN ECC X25519 PADA SHARED HOSTING PT APRILIA
TEKNOLOGI MANDIRI**

TUGAS AKHIR



Oleh :

RISQI RAHMAN PRATAMA

NIM : 2111510596

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR**

JAKARTA

2025

ABSTRAK

APLIKASI CHATTING DAN FILE SHARING BERBASIS WEB MENGUNAKAN HYBRID ENCRYPTION AES 256 GCM DAN ECC X25519 PADA SHARED HOSTING PT APRILIA TEKNOLOGI MANDIRI

Oleh : Risqi Rahman Pratama (2111510596)

Risiko kebocoran data dan kesalahan pengiriman informasi penting menjadi masalah dalam komunikasi internal di PT Aprillia Teknologi Mandiri, terutama karena penggunaan aplikasi pesan instan publik yang tidak memisahkan komunikasi pribadi dan pekerjaan secara jelas. Kondisi ini berpotensi menurunkan efisiensi kerja dan membahayakan kerahasiaan informasi strategis perusahaan. Untuk mengatasi permasalahan tersebut, penelitian ini merancang dan mengimplementasikan aplikasi web chat dan berbagi file yang mengintegrasikan metode *hybrid encryption*, yaitu kombinasi *Advanced Encryption Standard-256* dalam mode *Galois/Counter Mode* (AES-256-GCM) untuk enkripsi isi pesan dan *Elliptic Curve Cryptography* (ECC) X25519 untuk menghasilkan pasangan kunci *private key* dan *public key* untuk setiap pengguna dan *shared key* secara dinamis di *backend* dengan mengkombinasikan *private key* pengirim dan *public key* penerima. *Shared key* ini kemudian digunakan untuk enkripsi kunci AES. Aplikasi dikembangkan menggunakan Laravel 12.3.0, Livewire 3.2.6, dan PHP 8.3.1, dan dapat diakses melalui <https://aprilliateknologi.site/>. Sistem ini mendukung komunikasi *real-time* dengan menerapkan teknik *polling* serta teknik *chunking* dan *streaming* agar proses pengiriman file besar dapat berjalan efisien dan tidak terkena batas waktu eksekusi. Berdasarkan hasil pengujian, sistem ini terbukti berhasil menyediakan media komunikasi yang aman dan stabil, baik untuk pesan privat, grup, maupun pengiriman file hingga 41 *megabyte* (MB). Enkripsi menggunakan AES-GCM terbukti menjaga integritas data melalui *authentication tag* yang sesuai *test vector* dari GCM SPEC, dan implementasi ECC X25519 berhasil menghasilkan *shared key* yang sesuai dengan test vector RFC 7748. Seluruh fungsi berjalan tanpa *error*, membuktikan sistem siap digunakan untuk mendukung komunikasi internal organisasi berskala kecil hingga menengah.

Kata Kunci: *Hybrid Encryption*, AES-256-GCM, ECC X25519, *Chunking*, Keamanan Data.

DAFTAR ISI

LEMBAR PENGESAHAN	iii
ABSTRAK.....	iv
SURAT PERNYATAAN TIDAK PLAGIAT	v
KATA PENGANTAR	vi
DAFTAR TABEL	vii
DAFTAR GAMBAR	viii
DAFTAR SIMBOL	xi
DAFTAR ALGORITMA	xiii
DAFTAR ISI.....	xiv
BAB I.....	1
PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	2
1.3. Batasan Masalah	3
1.4. Tujuan Penelitian	3
1.5. Manfaat Penelitian	4
1.6. Sistematika Penulisan	4
BAB II.....	5
LANDASAN TEORI.....	5
2.1. Kriptografi	5
2.1.1. Pengertian Kriptografi	5
2.1.2. Aspek Keamanan Dalam Kriptografi.....	5
2.1.3. Elemen Dasar Kriptografi.....	6
2.1.4. Jenis-Jenis Kriptografi	6
2.2. Algoritma AES-256.....	7
2.2.1. Struktur dan Ekspansi Kunci pada AES-256	7
2.2.2. Transformasi Dasar AES.....	8
2.2.3. Proses Dekripsi AES	12
2.3. Mode Operasi AES-GCM.....	14

2.3.1. Definisi dan Konsep Umum AES-GCM.....	14
2.3.2. Komponen-Komponen Utama AES-GCM	15
2.3.3. Tahapan Proses Enkripsi dalam AES-GCM	15
2.3.4. GHASH dan GMAC	17
2.3.5. Pentingnya Keunikan <i>Initialization Vector</i> (IV)	18
2.4. <i>Elliptic Curve Cryptography</i> (ECC) dan X25519	18
2.4.1. Pengertian Umum ECC	19
2.4.2. Struktur Matematika Kurva Eliptik	19
2.4.3. Kurva yang Umum Digunakan dalam ECC	19
2.5. <i>Hybrid Encryption</i>	20
2.5.1. Pengertian <i>Hybrid Encryption</i>	21
2.5.2. Komponen dalam <i>Hybrid Encryption</i>	21
2.5.3. Cara Kerja <i>Hybrid Encryption</i>	21
2.6. <i>Chunking</i> dan <i>Streaming</i> file	22
2.6.1. Pengertian Umum	22
2.6.2. <i>Chunking</i> Dalam Sistem Enkripsi File.....	22
2.6.3. <i>Streaming</i> Untuk Proses Download Aman	23
2.7. Tinjauan Pustaka	23
BAB III	28
METODOLOGI PENELITIAN.....	28
3.1. Data Penelitian	28
3.2. Metode Pembandingan	28
3.3. Penerapan Metode.....	29
3.3.1. Penerapan Algoritma AES 256	30
3.3.2. Penerapan Mode Operasi AES-GCM	31
3.3.3. Penerapan Algoritma ECC X25519	36
3.3.4. Penerapan <i>Hybrid Encryption</i>	40
3.3.5. Penerapan <i>Chunking</i> File dan <i>Streaming</i> Download	43
3.4. Rancangan Pengujian.....	44
3.4.1. Pengujian Validasi Algoritma Kriptografi	44
3.4.2. Pengujian Fungsi Enkripsi dan Dekripsi File	45

3.4.3. Pengujian <i>Chunking</i> dan <i>Streaming</i>	45
3.4.4. Pengujian Komunikasi Real-time (Polling).....	45
3.4.5. Pengujian Performa Sistem.....	46
3.5. Rancangan Basis Data	46
3.5.1. Class Diagram Berdasarkan Struktur Basis Data	46
3.5.2. Logical Record Structure (LRS)	52
3.5.3. Spesifikasi Basis Data.....	55
3.6. Rancangan Menu	62
3.7. Rancangan Layar	63
3.7.1. Rancangan Layar Halaman Register.....	63
3.7.2. Rancangan Layar Halaman Login	64
3.7.3. Rancangan Layar Halaman Lupa Password	65
3.7.4. Rancangan Layar Halaman Home	66
3.7.5. Rancangan Layar Halaman Profil.....	66
3.7.6. Rancangan Layar Halaman Chat	67
BAB IV	69
HASIL DAN PEMBAHASAN.....	69
4.1. Lingkungan Percobaan	69
4.2. Implementasi Metode	70
4.2.1. Penerapan AES-256-GCM untuk Enkripsi Konten	70
4.2.2. Penerapan X25519 untuk Pertukaran Kunci.....	71
4.2.3. Penerapan <i>Chunking</i> File.....	71
4.2.4. Proses Dekripsi dan <i>Streaming</i> file.....	72
4.3. Flowchart	73
4.3.1. Flowchart Halaman Utama	73
4.3.2. Flowchart Halaman Register	75
4.3.3. Flowchart Halaman Login	77
4.3.4. Flowchart Halaman Profil.....	79
4.3.5. Flowchart Halaman Chatting	81
4.3.6. Flowchart Proses Enkripsi AES	82
4.3.7. Flowchart Enkripsi AES Mode GCM.....	84

4.3.8. Flowchart Pembuatan <i>Hash Sub Key</i>	85
4.3.9. Flowchart Enkripsi Plaintext dengan Mode Counter (CTR)	86
4.3.10. Flowchart Proses GHASH	87
4.3.11. Flowchart Pembuatan <i>Tag</i> Autentikasi	88
4.3.12. Flowchart <i>Decode Little Endian</i>	89
4.3.13. Flowchart <i>Encode Little Endian</i>	91
4.3.14. Flowchart <i>Clamping</i>	92
4.3.15. Flowchart <i>Conditional Swap</i> (CSWAP)	92
4.3.16. Flowchart <i>Montgomery Ladder Step</i>	93
4.3.17. Flowchart Proses <i>Scalar Multiplication</i> ECC X25519.....	95
4.4. Algoritma	97
4.4.1. Algoritma Halaman Utama	97
4.4.2. Algoritma Halaman Register	98
4.4.3. Algoritma Halaman Login	98
4.4.4. Algoritma Halaman Profil.....	99
4.4.5. Algoritma Halaman Chat	99
4.4.6. Algoritma Enkripsi CTR <i>Plain Text</i>	100
4.4.7. Algoritma Halaman <i>Hash Sub Key</i>	101
4.4.8. Algoritma Proses GHASH	101
4.4.9. Algoritma Pembuatan <i>Tag</i> Autentikasi	102
4.4.10. Algoritma <i>Decoding Little Endian</i>	103
4.4.11. Algoritma <i>Encoding Little Endian</i>	103
4.4.12. Algoritma <i>Clamping Private Key Generation</i>	103
4.4.13. Algoritma <i>Conditional Swap</i> (CSWAP)	104
4.4.14. Algoritma <i>Montgomery Ladder</i> ECC	104
4.4.15. Algoritma <i>Scalar Multiplication</i> ECC	105
4.5. Pengujian	106
4.5.1. Pengujian <i>Test Vector</i>	106
4.5.2. Pengujian Program.....	108
4.6. Analisis Pengujian.....	111
4.6.1. Analisa Pengujian Test Vector.....	111

4.6.2. Analisa Pengujian Test Program	112
4.7. Tampilan Layar Aplikasi	113
4.7.1. Tampilan Layar Halaman Register	113
4.7.2. Tampilan Layar Halaman Login	114
4.7.3. Tampilan Layar Halaman Lupa Password	115
4.7.4. Tampilan Layar Halaman Home	115
4.7.5. Tampilan Layar Terima File dan Unduh File Terenkripsi	116
4.7.6. Tampilan Layar Halaman Profil	117
4.7.7. Tampilan Layar Chat Pribadi	117
4.7.8. Tampilan Layar Chat Grup	118
4.7.9. Tampilan Layar Dekripsi file	119
BAB V	120
PENUTUP	120
5.1. Kesimpulan	120
5.2. Saran	121
DAFTAR PUSTAKA	122
LAMPIRAN	125

DAFTAR PUSTAKA

- Arif, Z., & Nurokhman, A. (2023). Analisis perbandingan algoritma kriptografi simetris dan asimetris dalam meningkatkan keamanan sistem informasi. *JTSI*, 4(2), pp. 395. <https://doi.org/10.35957/jtsi.v4i2.6077>
- Azhari, M., Mulyana, D. I., Perwitosari, J., & Ali, F. (2022). Implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains dan Komputer*, 2(1), pp. 163–166. <https://doi.org/10.47709/jpsk.v2i01.1390>
- Chen, L., Moody, D., Regenscheid, A., & Robinson, A. (2023). Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters (*NIST SP 800-186*). Gaithersburg, MD: National Institute of Standards and Technology. pp. 4-5 <https://doi.org/10.6028/NIST.SP.800-186>
- Donald, L. E., Phillip, J. B., & Karen, H. B. (2023). *Advanced Encryption Standard (AES) (FIPS 197: Federal Information Processing Standards Publication)*. New York: U.S. Department of Commerce, pp. 5-26. <https://doi.org/10.6028/NIST.FIPS.197-upd1>
- Dworkin, M. J. (2007). Recommendation for Block Cipher Modes of Operation. Gaithersburg (*NIST Special Publication 800-38D*). MD: National Institute of Standards and Technology, pp. 7-25. <https://doi.org/10.6028/NIST.SP.800-38d>
- Harahap, A. R., & Salim, T. A. (2023). Sistem kriptografi pada pengamanan autentikasi dokumen elektronik: Sistematic literature review. *Jurnal Pengembangan Kearsipan*, 16(2), pp. 210–211. <https://doi.org/10.22146/khazanah.81893>
- Hernandi, R. M., & Chandra, J. C. (2024). Implementasi algoritme AES-256 dan AES-GCM untuk mengamankan dokumen pada sistem data rekam medis Klinik Mulya. *KRESNA: Jurnal Riset dan Pengabdian Masyarakat*, 4(1), pp. 12–21. <https://doi.org/10.36080/kresna.v4i1.131>
- Jamaluddin, J., Saragih, N. F., Simamora, R. J., Siringoringo, R., & Purba, E. N. (2021). Konsep pengamanan video conference dengan enkripsi AES-GCM pada aplikasi Zoom. *Methomika: Jurnal Manajemen Informatika dan Komputerisasi Akuntansi*, 4(2), p. 111. <https://doi.org/10.46880/jmika>.
- Kafa, N. A., Virgiani, D., & Sakti, S. Y. (2024). Implementasi kriptografi berbasis web dengan algoritma Advanced Encryption Standard (AES) 256 dan kompresi Huffman untuk pengamanan file di SMK Satria. *Jurnal TICOM: Technology of*

Information and Communication, 12(2), p. 50.
<https://doi.org/10.70309/ticom.v12i2.109>

Kalan, R. S., & Dülger, I. (2024). A survey on QoE management schemes for HTTP adaptive video streaming: Challenges, solutions, and opportunities. *IEEE Access*, early access, pp. 1–2. <https://doi.org/10.1109/ACCESS.2024.3491613>

Kautsar, A., & Ikhsan, M. (2025). Implementasi algoritma Advanced Encryption Standard (AES) dan teknik steganografi Bit Plane Complexity Segmentation (BPCS) dalam eskalasi keamanan file teks. *Sistemasi: Jurnal Sistem Informasi*, 14(2), pp. 956–968 <http://sistemasi.ftik.unisi.ac.id>

Kristiadi, D., & Marwiyati. (2021). Adaptive streaming server dengan FFMPEG dan Golang. *Jurnal RESTI*, 5(3), pp. 413–420.
<https://doi.org/10.29207/resti.v5i3.2998>

Laravel. (2024). Queues: Job processing for time-consuming tasks and concurrency. *Laravel Documentation*. Available at: <https://laravel.com/docs/queues> [Accessed 25 Jul. 2025].

Langley, A., Hamburg, M., & Turner, S. (2016). *Elliptic Curves for Security*. [RFC 7748], pp. 4-14. <https://doi.org/10.17487/RFC7748>

Purwiko, D.P.P., Dewanta, F. & Afianti, F (2022). Analisa penggunaan Elliptic Curve Cryptography pada sistem autentikasi pada Internet of Things. *Jurnal Multinetics*, 8(1), 42–49. <https://doi.org/10.32722/multinetics.v8i1.4701>

Putri Iqlima, P., Rayyan, M., Alfansuri, R., & Lestari, I. (2025). Implementasi sistem keamanan data menggunakan algoritma kriptografi asimetris Elliptic Curve Cryptography (ECC) berbasis website. *Jurnal Ilmu Komputer (JIKUM)*, 1(1), pp. 10–18. <https://doi.org/10.62671/jikum.v1i1.37>

Rizky, P.A, & Soim, S. (2024). Implementasi algoritma kriptografi AES CBC untuk keamanan komunikasi data pada hardware. *Jurnal Resistor*, 3(1), pp. 71–78. <https://doi.org/10.31598/jurnalresistor.v7i2.1650>

Ruzis, S. F. (2019). Perbandingan kinerja teknologi *streaming* HTTP pseudostreaming dan DASH pada jaringan area kampus Gedung D dan E FILKOM UB. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 3(10), pp. 10130-10138. <http://j-ptiik.ub.ac.id>

Saputro, T. H., Hidayati, N., & Ujianto, E. I. H. (2020). Survei tentang algoritma kriptografi asimetris. *JIP (Jurnal Informatika Polinema)*, 10(10), pp. 67–72. <https://doi.org/10.33795/jip.v6i2.345>

- Swatrahadi, J., Permana, Hendrana, & Munir, R. (2024). Mengamankan file rahasia menggunakan hybrid kriptografi. *Jurnal Review Pendidikan dan Pengajaran*, 7(1), pp. 2449–2458. <https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/download/26156/18236/84755>
- Tanksale, V. (2024). Efficient elliptic curve Diffie–Hellman *key* exchange for resource-constrained IoT devices. *Electronics* (Switzerland), 13(18), p. 3. <https://doi.org/10.3390/electronics13183631>
- Tmeizeh, M.A., Rodríguez-Domínguez, C. & Hurtado-Torres, M.V. (2024) ‘File chunking towards on-chain storage: a blockchain-based data preservation framework’, *Cluster Computing*, 27(10), pp. 13531–13544. <https://doi.org/10.1007/s10586-024-04646-6>
- Widarma, A. (2023). Kombinasi algoritma simetri dan ECC untuk meningkatkan keamanan pesan. *Jurnal Nasional Informatika dan Teknologi Jaringan*, 8(1), pp. 1–5. <https://doi.org/10.30743/infotekjar.v8i1.9642>
- Widodo, B.E. & Purnomo, A.S., 2020. Implementasi *Advanced Encryption Standard* pada Enkripsi dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY. *Jurnal Teknik Informatika (JUTIF)*, 1(2), p. 71. <https://doi.org/10.20884/1.jutif.2020.1.2.21>
- William, C. J. (2023). Implementasi kriptografi hybrid dalam pengelolaan properti rahasia pada aplikasi Spring Boot (Makalah Tugas). Program Studi Teknik Informatika, STEI ITB. pp. 1-3 [https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/Makalah2/Makalah2-Kriptografi-2023%20\(13\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/Makalah2/Makalah2-Kriptografi-2023%20(13).pdf)
- Zhang, D., Chen, J., He, Y., Lan, X., Chen, X., Dong, C. & Li, J. (2023) ‘A chunked and disordered data privacy protection algorithm: application to resource platform systems’, *Applied Sciences*, 13(10), pp. 1-2. <https://doi.org/10.3390/app13106017>