

**PERANCANGAN DAN ANALISIS SISTEM KEAMANAN DOKUMEN
DIGITAL BERBASIS KRIPTOGRAFI HIBRIDA CAMELLIA-128 DAN
BLAKE3**



TUGAS AKHIR

**Disusun untuk Memenuhi Syarat Menyelesaikan Tugas Akhir Pendidikan
Sarjana Terapan pada Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi**

Oleh:

Putri Nabila

062240352316

**POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2026**

**PERANCANGAN DAN ANALISIS SISTEM KEAMANAN DOKUMEN
DIGITAL BERBASIS KRIPTOGRAFI HIBRIDA CAMELLIA-128 DAN
BLAKE3**



TUGAS AKHIR

**Disusun untuk Memenuhi Syarat Menyelesaikan Tugas Akhir Pendidikan
Sarjana Terapan pada Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi**

Oleh :

Nama	: Putri Nabila (062240352316)
Dosen Pembimbing I	: Ir. Aryanti,S.T., M.Kom., IPM.
Dosen Pembimbing II	: Martinus Mujur Rose, S.T., M.T.

**POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2026**

LEMBAR PENGESAHAN
PERANCANGAN DAN ANALISIS SISTEM KEAMANAN DOKUMEN
DIGITAL BERBASIS KRIPTOGRAFI HIBRIDA CAMELLIA-128 DAN
BLAKE3



TUGAS AKHIR

Disusun untuk Memenuhi Syarat Menyelesaikan Tugas Akhir Pendidikan
Sarjana Terapan pada Jurusan Teknik Elektro
Program Studi Teknik Telekomunikasi
Politeknik Negeri Sriwijaya

Oleh:

Putri Nabila

062240352316

Menyetujui,

Palembang, 14 Agustus 2026
Dosen Pembimbing II

Dosen Pembimbing I

Ir. Arvanti, S.T., M.Kom., IPM.
NIP. 197708092002122802

Martinus Majur Rose, S.T., M.T.
NIP. 197412022008121002

Mengetahui,

Ketua Jurusan Teknik Elektro

Koordinator Program Studi Sarjana
Terapan Teknik Telekomunikasi



Dr. Ir. Selamat Muslimin, S.T., M.Kom., IPM.
NIP. 197907222008011007

Mohammad Fadhli, S.Pd., M.T.
NIP. 199004032018031001

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan:

Nama	: Putri Nabila
Jenis Kelamin	: Perempuan
Tempat Tanggal Lahir	: Palembang, 15 Desember 2004
Alamat	: Jl M Husin, No.909, RT.012, RW.004, Kec. Alang-alang Lebar, Palembang
NIM	: 062240352316
Program Studi	: Sarjana Terapan Teknik Telekomunikasi
Jurusan	: Teknik Elektro
Judul Skripsi/Laporan Akhir/Tugas Akhir	: Perancangan dan Analisis Sistem Keamanan Dokumen Digital Berbasis Kriptografi Hibrida Camellia-128 dan BLAKE3

Menyatakan dengan sesungguhnya bahwa:

1. Skripsi/Laporan Akhir/Tugas Akhir ini adalah hasil karya saya sendiri serta bebas dari tindakan plagiasi dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.
2. Dapat menyelesaikan segala urusan terkait pengumpulan revisi Skripsi/Laporan Akhir yang sudah disetujui oleh dewan penguji paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.
3. Dapat menyelesaikan segala urusan peminjaman/penggantian alat buku dan lainnya paling lama 1 bulan setelah ujian Skripsi/Laporan Akhir.

Apabila dikemudian hari diketahui ada pernyataan yang terbukti tidak benar dan tidak dapat dipenuhi, maka saya siap bertanggung jawab dan menerima sanksi tidak diikutsertakan dalam prosesi wisuda serta dimasukkan dalam daftar hitam oleh jurusan Teknik Elektro sehingga berdampak tertundanya pengambilan Ijazah & Transkrip (ASLI & COPY). Demikian surat pernyataan ini dibuat dengan sebenar-benarnya dan dalam keadaan sadar tanpa paksaan.



Palembang, 14 Agustus 2026

Menyatakan

D5AAOX143811208 Putri Nabila)

MOTTO DAN PERSEMBAHAN

“Semua orang memiliki bahasanya sendiri.”

(Kim Yeong-hwan, *Can This Love Be Translated?*)

“Hidup seperti sebuah perjalanan. Ada saatnya kita harus berjalan melewati badai.”

(When Life Gives You Tangerines)

“Sesungguhnya bersama kesulitan ada kemudahan.”

(QS. Al-Insyirah: 6)

Tugas Akhir ini kupersembahkan kepada:

1. Abah dan Ibu, yang senantiasa menemani setiap proses perjalanan penulis. Terima kasih atas segala dukungan, doa, perhatian, serta pikiran-pikiran positif yang selalu diberikan sehingga penulis tetap semangat untuk terus melangkah dan menyelesaikan setiap proses yang ada.
2. Adik perempuanku, yang selalu memberikan dukungan kepada penulis. Terima kasih telah hadir dengan segala tingkah dan caramu sendiri yang mampu membuat suasana menjadi lebih baik di tengah proses yang tidak selalu mudah.
3. Bapak Muslimin dan keluarga, yang selalu memberikan motivasi, dukungan, dan dorongan kepada penulis untuk terus berkembang, melangkah lebih jauh, serta mempersiapkan diri untuk meraih kesuksesan di masa yang akan datang.
4. Ibu Ir. Aryanti, S.T., M.Kom., IPM. dan Bapak Martinus Mujur Rose, S.T., M.T. Terima kasih atas waktu, kesabaran, dan ilmu yang telah diberikan.
5. Teman-teman seperjuangan, terima kasih atas semangat, bantuan, kebersamaan, dan ilmu yang telah saling dibagikan selama menjalani proses perkuliahan hingga penyelesaian Tugas Akhir ini.
6. Diri sendiri, yang telah bertahan dan terus berusaha hingga sampai pada titik ini. Terima kasih karena telah memilih untuk tetap melangkah, berusaha percaya pada kemampuan diri sendiri, dan terus menanamkan pikiran positif untuk menghadapi setiap proses. Semoga langkah ini menjadi awal untuk terus berkembang dan berani melangkah lebih jauh ke depannya.

ABSTRAK

PERANCANGAN DAN ANALISIS SISTEM KEAMANAN DOKUMEN DIGITAL BERBASIS KRIPTOGRAFI HIBRIDA CAMELLIA-128 DAN BLAKE3

(2026 : xiv + 78 halaman + 22 gambar + 17 tabel + 9 lampiran)

PUTRI NABILA

062240352316

JURUSAN TEKNIK ELEKTRO

PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI
POLITEKNIK NEGERI SRIWIJAYA

Meningkatnya ancaman terhadap keamanan dokumen digital menyebabkan kebutuhan akan sistem yang mampu menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan dokumen digital berbasis web bernama SecureVault dengan mengintegrasikan algoritma Camellia-128 dan BLAKE3 menggunakan pendekatan kriptografi hibrida dengan skema *Hash-then-Encrypt*. Camellia-128 dalam mode CBC digunakan untuk mengenkripsi dokumen, sedangkan BLAKE3 diterapkan dalam proses pembentukan *secret key* dan mekanisme hashing. Sistem dibangun menggunakan arsitektur *client-server* dengan Vue 3 pada sisi *frontend*, Express.js dan Node.js pada sisi *backend*, serta MySQL sebagai penyimpanan metadata. Sistem juga dilengkapi autentikasi pengguna, pengelolaan dokumen, serta integrasi Telegram Bot API sebagai media distribusi *secret key* kepada pengguna yang telah menautkan akun Telegram. Pengujian dilakukan melalui pengujian fungsional, integritas file, *round-trip*, performa enkripsi dan dekripsi, serta integrasi Telegram. Hasil pengujian menunjukkan bahwa seluruh fungsi utama sistem berhasil dijalankan dengan tingkat keberhasilan 100%. Pengujian integritas menunjukkan bahwa file asli dan hasil dekripsi memiliki nilai SHA-256 yang identik, sedangkan file terenkripsi memiliki nilai hash yang berbeda. Pengujian *round-trip* pada file berukuran 531.072 *byte* berhasil mengembalikan file ke ukuran semula sebesar 531.072 *byte* tanpa kehilangan data. Evaluasi kinerja menunjukkan rata-rata waktu enkripsi sebesar 132,4 ms dan dekripsi sebesar 121,7 ms, sedangkan notifikasi melalui Telegram berhasil 100%. Hasil tersebut menunjukkan bahwa SecureVault mampu memberikan perlindungan terhadap kerahasiaan dan integritas dokumen digital serta menjalankan proses enkripsi dan dekripsi dengan performa yang baik.

Kata Kunci: Kriptografi hibrida, Camellia-128, BLAKE3, keamanan dokumen digital, enkripsi, hashing, integritas data.

ABSTRACT

DESIGN AND ANALYSIS OF A DIGITAL DOCUMENT SECURITY SYSTEM BASED ON CAMELLIA-128 AND BLAKE3 HYBRID CRYPTOGRAPHY

(2026 : xiv + 78 pages + 22 pictures + 17 tables + 9 attachments)

PUTRI NABILA

062240352316

ELECTRICAL ENGINEERING DEPARTMENT

***STUDY PROGRAM BACHELOR OF APPLIED TELECOMMUNICATION
ENGINEERING***

STATE POLYTECHNIC OF SRIWIJAYA

The increasing threats to digital document security have created a need for systems capable of preserving data confidentiality and integrity. This study aims to design and implement a web-based digital document security system called SecureVault by integrating the Camellia-128 and BLAKE3 algorithms using a hybrid cryptographic approach with a Hash-then-Encrypt scheme. Camellia-128 in CBC mode is used to encrypt documents, while BLAKE3 is applied in the secret key generation and hashing processes. The system was developed using a client-server architecture with Vue 3 on the frontend, Express.js and Node.js on the backend, and MySQL for metadata storage. The system also provides user authentication, document management, and Telegram Bot API integration as a medium for distributing the secret key to users who have linked their Telegram accounts. Testing was conducted through functional testing, file integrity testing, round-trip testing, encryption and decryption performance testing, and Telegram integration testing. The results showed that all main system functions achieved a 100% success rate. Integrity testing demonstrated that the original and decrypted files had identical SHA-256 values, while the encrypted file produced a different hash value. The round-trip test on a 531,072-byte file successfully restored the file to its original size of 531,072 bytes without data loss. Performance evaluation showed an average encryption time of 132.4 ms and an average decryption time of 121.7 ms, while Telegram notification delivery achieved a 100% success rate. These results demonstrate that SecureVault is capable of protecting the confidentiality and integrity of digital documents while providing good performance in the encryption and decryption processes.

Keywords: *Hybrid cryptography, Camellia-128, BLAKE3, digital document security, encryption, hashing, data integrity.*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, karunia, dan hidayah-Nya, sehingga penulis dapat menyelesaikan Laporan Tugas Akhir yang berjudul **“Perancangan dan Analisis Sistem Keamanan Dokumen Digital Berbasis Kriptografi Hibrida Camellia-128 dan BLAKE3”** dengan baik dan tepat waktu. Shalawat serta salam semoga selalu tercurah kepada Nabi Muhammad SAW yang telah membawa umat manusia dari masa kegelapan menuju era yang penuh dengan ilmu pengetahuan seperti saat ini.

Laporan Tugas Akhir ini disusun sebagai salah satu syarat untuk memenuhi kurikulum pada Jurusan Teknik Elektro Program Studi Sarjana Terapan Teknik Telekomunikasi di Politeknik Negeri Sriwijaya, dengan tujuan merancang dan menganalisis sistem keamanan dokumen digital berbasis web menggunakan kombinasi algoritma kriptografi Camellia-128 dan BLAKE3 untuk meningkatkan kerahasiaan serta integritas data. Dalam proses penyusunannya, penulis menyadari bahwa laporan ini tidak terlepas dari bantuan, bimbingan, dan dukungan berbagai pihak, sehingga penulis menyampaikan terima kasih kepada **Ibu Ir. Aryanti, S.T., M.Kom. IPM.** dan **Bapak Martinus Mujur, S.T., M.T.** selaku dosen pembimbing atas arahan dan bimbingan yang sangat berarti, serta kepada pihak-pihak lain yang telah membantu.

1. Allah SWT atas segala rahmat, karunia, dan kemudahan yang diberikan sehingga penulis dapat menyelesaikan laporan ini.
2. Bapak Ir. Irawan Rusnadi, M.T. selaku Ketua Direktur Politeknik Negeri Sriwijaya.
3. Bapak Dr. Ir. Selamat Muslimin, S.T., M.Kom. IPM. selaku Ketua Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
4. Ibu Lindawati, S.T., M.T.I. selaku Sekretaris Jurusan Teknik Elektro Politeknik Negeri Sriwijaya.
5. Bapak Mohammad Fadhli, S.Pd., M.T. selaku Koordinator Program Studi Sarjana Terapan Teknik Telekomunikasi Politeknik Negeri Sriwijaya.

6. Bapak/Ibu Dosen Program Studi Sarjana Terapan Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
7. Abah, ibu, dan adik tercinta yang selalu mendoakan, mendukung, serta memberi semangat tanpa henti kepada penulis. Terima kasih atas kasih sayang, pengorbanan, dan motivasi yang diberikan, sehingga penulis dapat menyelesaikan laporan ini dengan baik. Dukungan moral maupun materi tersebut menjadi kekuatan bagi penulis dalam melewati setiap proses dan tantangan selama penyusunan tugas akhir ini.
8. Teman-teman seperjuangan yang telah membantu dan memberikan motivasi dalam proses penyusunan laporan ini.
9. Nawwafi Fauziah Amalia, yang juga berjuang bersama penulis dalam melewati berbagai proses perkuliahan. Terima kasih telah menjadi teman berbagi cerita, dan selalu menemani di saat senang maupun sulit. Terima kasih untuk setiap tawa, semangat, dan kebersamaan yang membuat perjalanan ini terasa lebih ringan. Semoga kebersamaan dan cerita baik ini tetap berlanjut di setiap langkah kita ke depannya.
10. ENHYPEN, terima kasih telah menemani proses penulis melalui karya-karya yang selalu memberikan semangat dan energi positif. Terima kasih telah menjadi salah satu alasan penulis kembali bersemangat untuk terus maju dan menyelesaikan setiap proses yang ada.

Penulis menyadari bahwa laporan ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga laporan ini dapat bermanfaat bagi pembaca dan menjadi referensi bagi penelitian selanjutnya di bidang keamanan dokumen digital

Palembang, 2026

Penulis

DAFTAR ISI

LEMBAR PENGESAHAN	iii
SURAT PERNYATAAN	iv
MOTTO DAN PERSEMBAHAN.....	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian	5
1.6 Metode Penulisan	5
1.7 Sistematika Penulisan	6
BAB II TINJAUAN PUSTAKA.....	9
2.1 Keamanan Dokumen Digital.....	9
2.2 Kriptografi.....	9
2.3 Konsep Dasar Kriptografi	10
2.3.1 Enkripsi	10
2.3.2 Dekripsi	10
2.3.3 Hashing	11
2.4 Kriptografi Simetris dan <i>Block Cipher</i>	11
2.5 Algoritma Camellia-128.....	11
2.6 Fungsi Hash dan Algoritma BLAKE3	12
2.7 Kriptografi Hibrida.....	13
2.8 Software yang Mendukung	14
2.8.1 <i>Visual Studio Code</i> (VsCode).....	14
2.8.2 <i>HyperText Markup Language</i> (HTML).....	15
2.8.3 <i>JavaScript</i>	15
2.8.4 <i>MySQL</i>	16
2.8.5 <i>Node.js</i>	17
2.8.6 <i>Google Cloud Platform</i> (GCP).....	18
2.8.7 <i>API Bot Telegram</i>	19
2.9 <i>State of The Art</i>	19
BAB III METODOLOGI PENELITIAN	24
3.1 Kerangka Penelitian	24
3.2 Rancangan Penelitian	25
3.3 Identifikasi Masalah	27
3.4 Analisis Kebutuhan Sistem	27
3.5 Perancangan Sistem	30
3.5.1 <i>Arsitektur Sistem</i>	31
3.5.2 <i>Entity Relationship Diagram</i> (ERD).....	32

3.5.3 Diagram Alur Enkripsi dan Dekripsi.....	34
3.5.4 Peranan Fitur Notifikasi Kunci Rahasia melalui Bot Telegram	36
3.6 Implementasi Sistem	40
3.7 Alur Pengujian.....	41
3.7.1 Persiapan Pengujian	41
3.7.2 Pengujian Fungsional Sistem	42
3.7.3 Pengujian Enkripsi dan Dekripsi.....	42
3.7.4 Pengujian Integritas Data (Hashing)	42
3.7.5 Pengujian Keamanan.....	43
3.7.6 Pengujian Konsistensi Sistem	43
3.7.7 Parameter Pengujian.....	43
3.8 Parameter Evaluasi.....	44
3.8.1 Parameter Evaluasi Kinerja Sistem	44
3.8.2 Metode Evaluasi.....	44
BAB IV HASIL DAN PEMBAHASAN.....	46
4.1 Hasil Implementasi Sistem.....	46
4.1.1 Implementasi Modul Otentikasi Pengguna	46
4.1.2 Implementasi Modul <i>File Vault</i> Terenkripsi.....	47
4.1.3 Implementasi Modul Admin	48
4.1.4 Implementasi Proses Dekripsi File	49
4.1.5 Implementasi Data Base.....	49
4.1.6 Implementasi Modul Notifikasi Telegram	51
4.2 Konsep Perhitungan Manual	51
4.2.1 Pembentukan Secret Key	52
4.2.2 Padding PKCS#7.....	52
4.2.3 Perhitungan Manual Enkripsi Camellia-128-CBC.....	53
4.2.4 Perhitungan Manual Dekripsi Camellia-128-CBC	54
4.3 Implementasi Antarmuka <i>Website</i>	55
4.3.1 Halaman Daftar	55
4.3.2 Halaman Masuk (<i>Login</i>)	56
4.3.3 Halaman Enkripsi.....	57
4.3.4 Halaman Dashboard	59
4.3.5 Halaman Dekripsi.....	60
4.3.6 Halaman Manajemen Pengguna.....	61
4.3.7 Halaman Koneksi Telegram	62
4.4 Hasil Analisis Pengujian Sistem.....	63
4.4.1 Analisis Pengujian Fungsional	64
4.4.2 Analisis Keamanan Dokumen	65
4.4.3 Analisis Integritas File	66
4.4.4 Analisis <i>Round-Trip Crypto Service</i>	66
4.4.5 Analisis Pengujian Performa Sistem	67
4.4.6 Analisis Pengujian Notifikasi Telegram	69
4.5. Evaluasi Kinerja Sistem	70
BAB V PENUTUP	72
5.1 Kesimpulan	72
5.2 Saran.....	73
DAFTAR PUSTAKA.....	75
LAMPIRAN	

DAFTAR GAMBAR

Gambar 2. 1 Logo VsCode [16]	14
Gambar 2. 2 Logo HTML [18].....	15
Gambar 2. 3 Logo JavaScript [19]	15
Gambar 2. 4 Logo MySQL [22].....	16
Gambar 2. 5 Logo Node.js [24]	17
Gambar 2. 6 Logo Google Cloud Platform (CGP)	18
Gambar 3. 1 Kerangka Penelitian	24
Gambar 3. 2 Blok Diagram Rancangan Penelitian	26
Gambar 3. 3 Arsitektur Sistem.....	32
Gambar 3. 4 ERD SecureVault.....	32
Gambar 3. 5 Alur Enkripsi dan Dekripsi.....	34
Gambar 3. 6 Alur Penautan Akun Telegram	37
Gambar 3. 7 Alur Pengiriman Secret Key.....	39
Gambar 4. 1 Struktur Secret Key pada SecureVaultt	52
Gambar 4. 2 Halaman Daftar SecureVault	56
Gambar 4. 3 Halaman Login SecureVault.....	57
Gambar 4. 4 Halaman Enkripsi SecureVault.....	58
Gambar 4. 5 Halaman Dashboard SecureVault.....	59
Gambar 4. 6 Halaman Dekripsi SecureVault yang Berhasil	60
Gambar 4. 7 Halaman Dekripsi SecureVault yang Gagal	61
Gambar 4. 8 Halaman Manajemen Pengguna SecureVault	62
Gambar 4. 9 Halaman Koneksi Telegram	63

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	20
Tabel 3. 1 Kebutuhan Sistem Fungsional.....	28
Tabel 3. 2 Kebutuhan Non-Fungsional	29
Tabel 4. 1 Modul Otentikasi Pengguna	47
Tabel 4. 2 Modul File Vault Terenkripsi.....	48
Tabel 4. 3 Modul Admin	48
Tabel 4. 4 Struktur dari users	49
Tabel 4. 5 Struktur dari Files.....	50
Tabel 4. 6 Modul Notifikasi Telegram	51
Tabel 4. 7 Hasil Pengujian Fungsional.....	64
Tabel 4. 8 Hasil Pengujian Integritas File	66
Tabel 4. 9 Hasil Pengujian Round-Trip.....	66
Tabel 4. 10 Hasil Pengujian Waktu Enkripsi.....	67
Tabel 4. 11 Hasil Pengujian Waktu Dekripsi.....	68
Tabel 4. 12 Perbandingan Ukuran File.....	68
Tabel 4. 13 Hasil Pengujian Notifikasi Telegram	69
Tabel 4. 14 Evaluasi Kinerja Sistem	70

DAFTAR LAMPIRAN

Lampiran 1	Daftar Riwayat Hidup
Lampiran 2	Lembar Kesepakatan Bimbingan
Lampiran 3	Lembar Pelaksanaan Bimbingan
Lampiran 4	Lembar Rekomendasi Ujian Sidang Tugas Akhir
Lampiran 5	Lembar <i>Letter of Acceptance</i> Jurnal
Lampiran 6	Lembar Revisi Ujian Tugas Akhir
Lampiran 7	Lembar Pelaksanaan Revisi Ujian Tugas Akhir
Lampiran 8	Lembar Konfigurasi Coding
Lampiran 9	Dokumentasi