

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.