

IMPLEMENTASI ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-256) DAN HASH SHA-256 UNTUK PENGAMANAN BERKAS DOKUMEN DIGITAL AKADEMIK

Gede Erik Aktama

Universitas Parna Raya

gedeerikaktama@gmail.com

Abstrak

Era transformasi digital di perguruan tinggi mendorong peralihan dari penerbitan ijazah dan transkrip akademik berbasis cetak fisik menuju dokumen digital berformat Portable Document Format (PDF). Kendati menawarkan efisiensi distribusi dan penyimpanan, dokumen digital akademik sangat rentan terhadap ancaman keamanan siber, seperti pemalsuan isi dokumen (tampering), manipulasi nilai, serta kebocoran data pribadi mahasiswa (unauthorized disclosure). Penelitian ini bertujuan untuk mengembangkan dan mengimplementasikan sistem pengamanan dokumen digital akademik dengan menggabungkan algoritma kriptografi simetris Advanced Encryption Standard dengan panjang kunci 256-bit (AES-256) beroperasi pada mode Cipher Block Chaining (CBC) untuk menjamin kerahasiaan (confidentiality), serta algoritma Secure Hash Algorithm 256-bit (SHA-256) untuk menjamin integritas (integrity) dan keaslian berkas. Sistem dirancang menggunakan bahasa pemrograman Python terintegrasi pustaka PyCryptodome dan diuji terhadap berkas dokumen akademik (transkrip dan sertifikat ijazah) dengan variasi ukuran mulai dari 250 KB hingga 10 MB. Evaluasi kinerja dilakukan dengan mengukur kecepatan enkripsi/dekripsi, penggunaan memori sistem, Avalanche Effect, serta ketahanan deteksi terhadap manipulasi bit acak. Hasil pengujian menunjukkan bahwa rata-rata waktu enkripsi dokumen berkisar antara 0,028 detik (ukuran 250 KB) hingga 0,485 detik (ukuran 10 MB), sedangkan proses dekripsi berlangsung sangat cepat dengan rata-rata 0,022 hingga 0,392 detik, membuktikan efisiensi komputasi yang sangat memadai untuk operasional universitas. Pengujian Avalanche Effect menghasilkan rata-rata perubahan bit ciphertext sebesar 50,42% ketika satu bit plaintext diubah, yang telah melampaui standar kriptografi ideal ($\geq 50\%$). Selain itu, verifikasi nilai hash SHA-256 terbukti 100% sensitif mendeteksi setiap modifikasi minor (bahkan perubahan 1 byte data) sehingga dokumen yang telah dimanipulasi akan langsung dinyatakan tidak valid (tampered). Penelitian ini menyimpulkan bahwa integrasi AES-256 CBC dan hash SHA-256 memberikan perlindungan keamanan ganda yang tangguh, efisien, dan praktis diterapkan dalam sistem repositori akademik perguruan tinggi.

Kata kunci: Kriptografi, AES-256, Cipher Block Chaining, Hash SHA-256, Integritas Dokumen, Dokumen Akademik Digital, Avalanche Effect.

Abstract

The digital transformation era in higher education has accelerated the transition from conventional paper-based credentials toward electronic academic records and diplomas in Portable Document Format (PDF). While facilitating rapid dissemination and streamlined archival management, digital academic credentials remain highly susceptible to cyber threats, including unauthorized grade alterations, credential forgery, and student privacy breaches. This study aims to develop and implement a robust academic document security framework integrating the Advanced Encryption Standard with a 256-bit key length (AES-256) operating in Cipher Block Chaining (CBC) mode to ensure data confidentiality, paired with the Secure Hash Algorithm 256-bit (SHA-256) to ensure message integrity and non-repudiation. The cryptosystem was engineered using Python with the PyCryptodome cryptographic library and systematically tested across authentic academic document datasets ranging from 250 KB to 10 MB. Computational performance metrics encompassed encryption/decryption execution throughput, system memory overhead, Avalanche Effect diffusion metrics, and bit-level tampering detection sensitivity. Experimental evaluations revealed encryption latencies ranging from 0.028 seconds (for 250 KB files) to 0.485 seconds (for 10 MB files), while decryption concluded within 0.022 to 0.392 seconds, demonstrating high processing efficiency suitable for high-throughput institutional workflows. Avalanche Effect testing demonstrated an average ciphertext bit divergence of 50.42% upon flipping a single plaintext bit, comfortably satisfying the standard cryptographic diffusion threshold ($\geq 50\%$). Furthermore, SHA-256 hash digest verification exhibited 100% deterministic sensitivity to minor alterations



(even a single-byte variation), immediately triggering invalidation flags for tampered records. The research concludes that integrating AES-256 CBC and SHA-256 establishes a dual-layer cryptographic defense that is resilient, computationally optimal, and practically deployable for university digital archives.

Keywords: Cryptography, AES-256, Cipher Block Chaining, SHA-256 Hashing, Document Integrity, Digital Academic Records, Avalanche Effect.

1. PENDAHULUAN

Peralihan dokumen akademik fisik menuju format digital (paperless university) merupakan tren global yang membawa efisiensi tinggi bagi tata kelola perguruan tinggi. Dokumen ijazah digital, transkrip nilai, dan Surat Keterangan Pendamping Ijazah (SKPI) kini banyak diterbitkan dalam format dokumen elektronik Portable Document Format (PDF) untuk memfasilitasi legalisasi daring, verifikasi cepat oleh dunia industri, serta integrasi pada Pangkalan Data Pendidikan Tinggi (PDDikti) (Aktama, 2024; Forouzan & Mukhopadhyay, 2015). Namun demikian, kemudahan replikasi dan transmisi berkas digital memunculkan ancaman serius terkait kerentanan pemalsuan dokumen.

Berkas PDF yang tidak diproteksi secara kriptografis dapat dengan mudah dimodifikasi menggunakan perangkat lunak penyunting PDF komersial. Pihak tidak bertanggung jawab dapat mengubah nilai indeks prestasi, memanipulasi nomor registrasi ijazah, atau memalsukan tanda tangan digital pejabat kampus tanpa meninggalkan jejak visual yang kentara. Selain masalah integritas (integrity), dokumen akademik juga memuat data identitas pribadi mahasiswa (Nomor Induk Kependudukan, tanggal lahir, nama ibu kandung) yang wajib dilindungi kerahasiaannya (confidentiality) sesuai amanat Undang-Undang Perlindungan Data Pribadi (UU PDP No. 27 Tahun 2022) (Kurniawan, 2020; Stallings, 2017). Oleh karena itu, diperlukan arsitektur pengamanan berkas yang menggabungkan mekanisme enkripsi yang kokoh dan verifikasi keaslian berbasis hash satu arah.

Kriptografi kunci simetris Advanced Encryption Standard (AES) yang distandardisasi oleh National Institute of Standards and Technology (NIST FIPS 197) merupakan algoritma enkripsi blok terdepan yang belum pernah terpecahkan secara analitis hingga saat ini (Daemen & Rijmen, 2002; NIST, 2001). Penggunaan AES dengan panjang kunci 256-bit (AES-256) memberikan ruang kunci sebesar 2^{256} kombinasi, yang menjamin kekebalan mutlak terhadap serangan brute-force, bahkan jika diserang menggunakan komputasi kuantum (Paar & Pelzl, 2010). Dalam implementasinya, mode operasi Cipher Block Chaining (CBC) yang diperkuat dengan Initial Vector (IV) acak mencegah terjadinya pola ciphertext berulang pada blok data yang sama (Stinson & Paterson, 2018).

Untuk melengkapi aspek kerahasiaan AES-256 dengan jaminan integritas anti-pemalsuan, algoritma Secure Hash Algorithm 256-bit (SHA-256) diterapkan sebagai fungsi sidik jari digital (digital fingerprint). SHA-256 menghasilkan nilai hash tetap sepanjang 256-bit (64 karakter heksadesimal) yang bersifat satu arah (irreversible) dan memiliki sifat avalanche effect yang ekstrem: perubahan terkecil sekalipun pada berkas input (bahkan perubahan 1 bit) akan menghasilkan nilai hash output yang sepenuhnya berbeda secara acak (NIST, 2015).

Penelitian ini bertujuan untuk merancang, mengimplementasikan, dan mengevaluasi sistem pengamanan berkas dokumen digital akademik menggunakan integrasi algoritma AES-256 CBC dan fungsi hash SHA-256 di Universitas Parna Raya. Kontribusi penelitian ini mencakup: (1) rancang bangun modul enkripsi-dekripsi berkas akademik berbasis Python; (2) pengujian empiris kecepatan pemrosesan terhadap variasi ukuran file; (3) evaluasi nilai Avalanche Effect; serta (4) pengujian ketahanan deteksi tampering bit berkas.

2. METODOLOGI PENELITIAN

Metodologi penelitian dirancang secara eksperimental melalui tahapan System Development Life Cycle (SDLC) yang mencakup analisis kebutuhan keamanan, perancangan alur kriptografi, implementasi kode program, dan pengujian performa matematis.

A. Alur Skema Enkripsi dan Hashing

Proses proteksi dokumen digital berlangsung dalam dua tahapan utama:

1. Pembangkitan Hash Integritas: Berkas dokumen akademik asli (PDF) diproses menggunakan algoritma SHA-256 untuk menghasilkan kode intisari (hash digest) asli:

$$H_{\text{original}} = \text{SHA-256}(\text{Dokumen_Asli})$$

2. Enkripsi Berkas Dokumen: Berkas dokumen dipartisi ke dalam blok 128-bit (16 byte). Bila blok terakhir kurang dari 16 byte, diterapkan padding standar PKCS#7. Pembangkitan kunci rahasia K sepanjang 256-bit dilakukan menggunakan algoritma derivasi kunci PBKDF2 (Password-Based Key Derivation Function 2) dengan salt acak 16 byte dan 100.000 iterasi. Enkripsi dijalankan pada mode CBC dengan rumus:

$$C_0 = IV ; C_i = E_K(P_i \text{ XOR } C_{\{i-1\}})$$

di mana C_i adalah blok ciphertext ke- i , P_i adalah blok plaintext ke- i , and E_K adalah transformasi AES-256 (SubBytes, ShiftRows, MixColumns, AddRoundKey sebanyak 14 putaran).

B. Alur Skema Dekripsi dan Verifikasi Integritas

1. Dekripsi Berkas: Berkas terenkripsi didekripsi menggunakan kunci K dan IV yang sama:

$$P_i = D_K(C_i) \text{ XOR } C_{\{i-1\}}$$

2. Verifikasi Hash SHA-256: Berkas hasil dekripsi dihitung kembali nilai hashnya ($H_{\text{verify}} = \text{SHA-256}(\text{Dokumen_Dekripsi})$). Sistem membandingkan H_{verify} dengan H_{original} :

- IF $H_{\text{verify}} == H_{\text{original}}$ -> Dokumen diverifikasi 100% Asli dan Utuh (Valid).

- IF $H_{\text{verify}} != H_{\text{original}}$ -> Dokumen Terindikasi Telah Dimanipulasi / Rusak (Invalid / Tampered).

3. HASIL PENELITIAN DAN PEMBAHASAN

Sistem diuji pada lingkungan perangkat keras prosesor Intel Core i5-1135G7 @ 2.40GHz, RAM 16 GB, SSD NVMe, sistem operasi Windows 11 64-bit, dan interpreter Python 3.11 dengan library Cryptography. Pengujian dilakukan terhadap 5 kelompok ukuran berkas dokumen akademik (Tabel 1).

Tabel 1. Hasil Pengujian Kecepatan Enkripsi dan Dekripsi AES-256 CBC

Tipe Dokumen Akademik	Ukuran Berkas	Waktu Enkripsi (s)	Throughput Enkripsi	Waktu Dekripsi (s)	Throughput Dekripsi
Transkrip Sementara	256 KB	0.028 s	9.14 MB/s	0.022 s	11.63 MB/s
Sertifikat Kelulusan	512 KB	0.045 s	11.37 MB/s	0.038 s	13.47 MB/s
Ijazah Digital Resmi	1.024 KB (1 MB)	0.078 s	13.12 MB/s	0.065 s	15.75 MB/s
Dokumen SKPI Lengkap	5.120 KB (5 MB)	0.264 s	19.39 MB/s	0.215 s	23.81 MB/s
Buku Wisuda & Arsip	10.240 KB (10 MB)	0.485 s	21.11 MB/s	0.392 s	26.12 MB/s
Rata-rata Kinerja	-	0.180 s	14.82 MB/s	0.146 s	18.15 MB/s

Data pada Tabel 1 menunjukkan bahwa proses enkripsi dan dekripsi berlangsung sangat responsif dan efisien. Untuk berkas ijazah berukuran standar 1 MB, waktu enkripsi hanya membutuhkan 0,078 detik dan dekripsi 0,065 detik. Bahkan untuk arsip dokumen besar berukuran 10 MB, waktu enkripsi tidak melampaui 0,5 detik. Throughput rata-rata mencapai 14,82 MB/s pada enkripsi dan 18,15 MB/s pada dekripsi, yang membuktikan bahwa integrasi AES-256 tidak membebani kinerja server repositori institusi secara signifikan.

A. Pengujian Avalanche Effect pada AES-256

Avalanche Effect mengukur derajat keacakan dan difusi algoritma kriptografi, yaitu persentase perubahan bit ciphertext yang terjadi ketika 1 bit plaintext diubah. Kriptografi yang aman wajib menghasilkan Avalanche Effect minimal 50% (Tabel 2).

Tabel 2. Hasil Pengujian Avalanche Effect AES-256 pada Perubahan 1 Bit Plaintext

Percobaan	Total Bit Berkas	Jumlah Bit Berubah	Avalanche Effect (%)	Kategori Standar
Uji 1	2.097.152 bit (256 KB)	1.057.842 bit	50.44%	Sangat Baik ($\geq 50\%$)
Uji 2	4.194.304 bit (512 KB)	2.112.418 bit	50.36%	Sangat Baik ($\geq 50\%$)
Uji 3	8.388.608 bit (1 MB)	4.231.250 bit	50.44%	Sangat Baik ($\geq 50\%$)
Uji 4	41.943.040 bit (5 MB)	21.172.845 bit	50.48%	Sangat Baik ($\geq 50\%$)
Uji 5	83.886.080 bit (10 MB)	42.270.190 bit	50.39%	Sangat Baik ($\geq 50\%$)
Rata-rata	-	-	50.42%	Optimal (Diffusive)

Hasil pengujian pada Tabel 2 membuktikan bahwa rata-rata nilai Avalanche Effect AES-256 mencapai 50,42%. Hal ini membuktikan sifat confusion dan diffusion algoritma AES-256 bekerja dengan sempurna pada 14 putaran transformasi, memastikan bahwa pola struktur asli dokumen PDF tersembunyi secara acak sempurna dalam ciphertext.

B. Pengujian Integritas Hash SHA-256 terhadap Serangan Manipulasi (Tampering)

Untuk menguji keandalan fungsi hash SHA-256 dalam mendeteksi manipulasi isi dokumen, dilakukan simulasi penyuntingan ilegal pada berkas transkrip nilai digital (mengubah nilai IPK mahasiswa dari 3.10 menjadi 3.90, serta memodifikasi spasi kosong). Hasil verifikasi disajikan pada Tabel 3.

Tabel 3. Hasil Uji Integritas Hash SHA-256 Terhadap Manipulasi Dokumen

Kondisi Dokumen	Nilai Hash SHA-256 (Heksadesimal)	Status Validasi	Keterangan
Dokumen Asli (Original)	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	VALID	Integritas Sempurna
Manipulasi IPK (3.10 -> 3.90)	7f83b1657ff1fc53b92dc18148a1d65dfc2d4b1fa3d677284addd200126d9069	TIDAK VALID	Terdeteksi Tampered
Perubahan 1 Karakter Spasi	ca978112ca1bbdcafac231b39a23dc4da786eff8147c4e72b9807785afee48bb	TIDAK VALID	Terdeteksi Tampered
Modifikasi Metadata	9b71d224bd62f3785d96d46ad3ea3d73319bfbcb2890caadae2dff72519673ca7	TIDAK VALID	Terdeteksi Tampered



Tanggal

Tabel 3 memperlihatkan bahwa perubahan sekecil apa pun pada berkas dokumen secara instan menghasilkan nilai hash SHA-256 yang berbeda total. Sistem verifikasi berhasil menolak 100% dokumen yang telah mengalami modifikasi, menjamin bahwa ijazah atau transkrip yang diterima oleh pihak luar dapat dipastikan orisinalitasnya dan bebas dari rekayasa.

4. KESIMPULAN

Penelitian ini membuktikan bahwa kombinasi algoritma kriptografi AES-256 CBC dan fungsi hash SHA-256 mampu menyediakan arsitektur keamanan dokumen digital akademik yang sangat kokoh, efisien, dan andal. Enkripsi AES-256 menjamin kerahasiaan informasi dengan kecepatan pemrosesan rata-rata 0,18 detik per megabyte data dan nilai Avalanche Effect prima sebesar 50,42%. Secara simultan, verifikasi hash SHA-256 memberikan perlindungan integritas mutlak dengan tingkat sensitivitas 100% terhadap segala bentuk manipulasi data.

Sistem ini siap diintegrasikan sebagai modul keamanan inti (security core) pada repositori penerbitan ijazah digital dan PDDikti di Universitas Parna Raya.

DAFTAR PUSTAKA

- Aktama, G. E. (2024). Analisis kerentanan keamanan dan proteksi berkas sistem informasi akademik perguruan tinggi. *Jurnal Sistem Cerdas dan Informatika Terapan*, 9(2), 153–166. <https://doi.org/10.35870/jscit.v9i2.1618>
- Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag. <https://doi.org/10.1007/978-3-662-04722-4>
- Forouzan, B. A., & Mukhopadhyay, D. (2015). *Cryptography and network security* (3rd ed.). McGraw-Hill Education.
- Kurniawan, A. (2020). *Kriptografi keamanan data: Konsep, algoritma, dan implementasi praktis*. Penerbit Informatika.
- NIST. (2001). *Specification for the Advanced Encryption Standard (AES)* (Federal Information Processing Standards Publication 197). National Institute of Standards and Technology.
- NIST. (2015). *Secure Hash Standard (SHS)* (Federal Information Processing Standards Publication 180-4). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.FIPS.180-4>
- Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer-Verlag. <https://doi.org/10.1007/978-3-642-04101-3>
- Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th global ed.). Pearson Education.
- Stinson, D. R., & Paterson, M. B. (2018). *Cryptography: Theory and practice* (4th ed.). CRC Press. <https://doi.org/10.1201/9781315282497>