

# **ANALISIS PERBANDINGAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) 128, 192, DAN 256 BIT DALAM KEAMANAN DATA DIGITAL**

Putra Daffa Dwiyansah - 20230801432



# PENDAHULUAN

- Keamanan data merupakan aspek fundamental dalam sistem informasi modern.
- Peningkatan transaksi digital menyebabkan risiko tinggi terhadap kebocoran data dan serangan siber (Hidayatulloh et al., 2023).
- Kriptografi digunakan untuk menjaga kerahasiaan, integritas, dan autentikasi data.
- AES dikembangkan oleh Vincent Rijmen dan Joan Daemen, disetujui NIST pada tahun 2001 sebagai pengganti DES.
- Tiga varian utama AES:
  1. AES-128
  2. AES-192
  3. AES-256
- Tujuan: menganalisis dan membandingkan performa serta keamanan dari ketiga varian berdasarkan penelitian terdahulu.



# **TUJUAN LITERATURE REVIEW**

1. Menjelaskan konsep dasar kriptografi dan algoritma AES.
2. Menganalisis hasil penelitian sebelumnya mengenai perbandingan AES-128, 192, dan 256.
3. Menentukan arah dan peluang penelitian lanjutan dalam implementasi AES pada sistem modern seperti web dan cloud.

# KONSEP DASAR KRIPTOGRAFI DAN AES

Menurut Hidayatulloh et al. (2023):  
Kriptografi adalah teknik penyandian pesan agar hanya pihak berwenang yang dapat membaca.

Tujuan utama:

- Confidentiality (Kerahasiaan)
- Integrity (Integritas data)
- Authentication (Keaslian)
- Non-repudiation (Tidak dapat disangkal)

Jenis utama algoritma:

- Simetris → AES, DES, Blowfish
- Asimetris → RSA, ECC
- Hash → SHA, MD5

Algoritma AES (Advanced Encryption Standard)  
Merupakan algoritma kriptografi simetris berbasis blok 128-bit.

Memiliki tiga panjang kunci dan jumlah ronde berbeda:

- AES-128 → 10 ronde
- AES-192 → 12 ronde
- AES-256 → 14 ronde (Tampubolon et al., 2014)

Tahapan utama proses:

1. SubBytes
2. ShiftRows
3. MixColumns
4. AddRoundKey

# TINJAUAN BEBERAPA PENELITIAN TERDAHULU TENTANG AES

- [1] Hidayatulloh et al. (2023)  
Menjelaskan dasar konsep AES, struktur matematis, dan ketahanannya terhadap serangan brute-force. Menegaskan perbedaan antar varian AES dari jumlah ronde dan kekuatan kunci.
- [2] Kusyanti & Amron (2018)  
Membandingkan tiga varian AES pada Android:
  - AES-128 tercepat,
  - AES-192 seimbang,
  - AES-256 paling aman namun lambat.Rekomendasi: pilih berdasarkan kebutuhan sistem efisiensi atau keamanan.
- [3] Santoso & Rahman (2022)  
Implementasi AES-128 pada enkripsi dokumen Android.
  - Cepat dan efisien, cocok untuk perangkat mobile.
  - Tidak membandingkan dengan AES-192/256.
- [4] Tampubolon et al. (2014)  
Uji AES-128, 192, 256 pada file multimedia.
  - Semakin panjang kunci → keamanan naik, waktu proses bertambah 20–30%.
  - AES-192 paling seimbang antara kecepatan dan keamanan.
- [5] Indrayani, Ferdiansyah, & Koprawi (2025)  
Fokus pada AES-256 untuk file berbagai format (teks, audio, video).
  - Keamanan sangat tinggi dan menjaga integritas data.
  - Waktu enkripsi lebih lama dibanding varian lain.

# ANALISIS DAN SINTESIS

## Analisis Hasil Penelitian

- Semakin panjang kunci AES, semakin tinggi tingkat keamanan, tetapi waktu enkripsi juga meningkat.
- AES-128: Paling cepat dan efisien, Ideal untuk perangkat mobile dan real-time system (Santoso & Rahman, 2022).
- AES-192: Keseimbangan performa dan keamanan (Kusyanti & Amron, 2018; Tampubolon et al., 2014).
- AES-256: Keamanan tertinggi, ideal untuk sistem cloud dan database sensitif (Indrayani et al., 2025).

## Research Gap:

1. Belum ada analisis komprehensif terkait konsumsi energi dan memori.
2. Minim kajian penggunaan hardware acceleration (AES-NI).
3. Belum banyak penelitian terkait side-channel attack.



# ARAH DAN PELUANG PENELITIAN

Berdasarkan hasil kajian, arah penelitian selanjutnya:

1. Implementasi AES-256 pada framework web seperti Laravel dan Filament.
2. Field-level encryption pada database untuk meningkatkan keamanan data sensitif.
3. Uji empiris perbandingan efisiensi AES-128, 192, dan 256 pada server web.
4. Analisis CPU usage, throughput, dan efisiensi energi.



# KESIMPULAN

- Semua varian AES memiliki tingkat keamanan tinggi.
- AES-128: unggul dalam kecepatan dan efisiensi sumber daya.
- AES-192: seimbang antara performa dan keamanan.
- AES-256: keamanan paling tinggi, cocok untuk data sensitif.
- Pemilihan varian bergantung pada kebutuhan sistem dan konteks aplikasi.



# DAFTAR PUSTAKA

Hidayatulloh, N. W., Tahir, M., Amalia, H., Afdlolul Basyar, N., Faizal Prianggara, A., & Yasin, M. (2023). Mengenal Advanced Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data. *Digital Transformation Technology (Digitech)*, 3(1), 1–10.  
Link: <https://jurnal.itscience.org/index.php/digitech/article/view/2293>

Kusyanti, A., & Amron, K. (2018). Analisis Perbandingan Algoritma Advanced Encryption Standard untuk Enkripsi Short Message Service (SMS) pada Android. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(10), 4281–4289.

Link: <https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/2893/1112>

Santoso, T. B., & Rahman, F. H. (2022). Analisa dan Perancangan Sistem Enkripsi dan Dekripsi Dokumen Berbasis Android Menggunakan Metode Advanced Encryption Standard-128 (Studi Kasus: PT. Kelab 21 Retail). *Jurnal Logika dan Manajemen Teknologi (JLMT)*, 2(1), 45–53.

Link: <https://ojs-teknik.usni.ac.id/index.php/jlmt/article/view/197>

Tampubolon, N. B., Isnanto, R. R., & Sinuraya, E. W. (2014). Implementasi dan Analisis Algoritma Advanced Encryption Standard (AES) pada Tiga Variasi Panjang Kunci untuk Berkas Multimedia. *Jurnal Transient*, Universitas Diponegoro, 3(4), 567–574.

Link: <https://ejournal3.undip.ac.id/index.php/transient/article/view/10581>

Indrayani, R., Ferdiansyah, P., & Koprawi, M. (2025). Analisis Penggunaan Kriptografi Metode AES 256 Bit pada Pengamanan File dengan Berbagai Format. *Digital Transformation Technology*, 4(2), 1245–1251.  
Link: <https://jurnal.itscience.org/index.php/digitech/article/view/5457>

**THANK YOU FOR**



**ATTENTION**