



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

Putra Daffa Dwiyansah - 20230801432
Fiqri Fathurrohman - 20230801209
Nakhwah Alfikry - 20230801244



LATAR BELAKANG MASALAH

- Pertukaran data digital yang semakin masif meningkatkan risiko kebocoran dan manipulasi data.
- Kriptografi berperan penting dalam menjaga kerahasiaan dan integritas informasi digital.
- Advanced Encryption Standard (AES) merupakan algoritma kriptografi simetris yang digunakan secara luas.
- AES memiliki tiga varian kunci (128, 192, dan 256 bit) dengan karakteristik keamanan dan performa yang berbeda.
- Belum semua sistem memahami implikasi pemilihan varian AES terhadap efisiensi dan keamanan.



TUJUAN DAN RUANG LINGKUP PEMBAHASAN

Tujuan Penelitian:

- Menganalisis perbedaan performa dan tingkat keamanan AES-128, AES-192, dan AES-256.
- Mengidentifikasi trade-off antara efisiensi komputasi dan kekuatan enkripsi.
- Memberikan dasar pemilihan varian AES sesuai kebutuhan sistem.

Ruang Lingkup Pembahasan:

- Panjang kunci dan jumlah ronde enkripsi
- Waktu pemrosesan dan efisiensi sumber daya
- Ketahanan terhadap ancaman keamanan



HASIL PEMBAHASAN UTAMA

Performa dan Efisiensi:

- AES-128
 - Waktu enkripsi tercepat
 - Konsumsi CPU dan memori paling rendah
 - Cocok untuk perangkat mobile dan sistem real-time
- AES-192
 - Performa menengah
 - Beban komputasi lebih tinggi dari AES-128
 - Jarang digunakan dalam praktik
- AES-256
 - Waktu pemrosesan paling lama
 - Beban sumber daya tertinggi
 - Efektif untuk data berukuran besar dan sensitif

Keamanan:

- Keamanan meningkat seiring bertambahnya panjang kunci
- AES-256 paling tahan terhadap brute-force attack



KESIMPULAN DAN IMPLIKASI

Kesimpulan:

- AES-128 unggul dalam efisiensi dan kecepatan
- AES-192 menawarkan keseimbangan performa dan keamanan
- AES-256 unggul dalam keamanan jangka panjang

Implikasi Penggunaan:

- Pemilihan varian AES harus disesuaikan dengan:
 - Sensitivitas data
 - Kapasitas sistem
 - Konteks aplikasi



THANK YOU FOR
ATTENTION