KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Research Student
Vol.2, No.2 September 2025
e-ISSN: 3025-5694; p-ISSN: 3025-5708, Hal 917-923
DOI: https://doi.org/10.61722/jirs.v2i2.5908

Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish

Zefanya Seto Gandhara
Universitas Pertahanan Republik Indonesia
Tegar Pandu Satria
Universitas Pertahanan Republik Indonesia
Hondor Saragih
Universitas Pertahanan Republik Indonesia
Muhammad Naufal Nafian Abror
Universitas Pertahanan Republik Indonesia

Alamat: Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810
Korespondensi penulis: zefanyaseto@gmail.com

Abstract. *Digital data security is increasingly becoming a major concern in the modern era, especially in securing video files containing important information. One method commonly used to protect video data is cryptography which aims to convert the original data into an encrypted form so that it cannot be accessed by unauthorized parties. A comparison was made between three popular cryptographic algorithms, namely Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Blowfish, in the process of video encryption and decryption. This study analyzes the performance of the three algorithms based on processing time, resource consumption, security of encryption results and storage efficiency. The evaluation results show that AES has a high level of security but requires a longer processing time compared to Blowfish. DES shows weaknesses in terms of security due to its smaller key size, making it more vulnerable to cryptographic attacks. Blowfish offers a balance between processing speed and security, making it an efficient choice for video security with better performance than DES. It is expected to provide recommendations on the most optimal algorithm to use in digital video security both in terms of time efficiency, resource consumption and security level.*

Keywords: *Cryptography, AES, DES, Blowfish, Video Encryption*.

Abstrak. Keamanan data digital semakin menjadi perhatian utama di era modern, terutama dalam pengamanan file video yang berisi informasi penting. Salah satu metode yang umum digunakan untuk melindungi data video adalah kriptografi yang bertujuan untuk mengubah data asli menjadi bentuk terenkripsi agar tidak dapat diakses oleh pihak yang tidak berwenang. Dilakukan perbandingan antara tiga algoritma kriptografi populer, yaitu Advanced Encryption Standard (AES), Data Encryption Standard (DES), dan Blowfish, dalam proses enkripsi dan dekripsi video. Penelitian ini menganalisis performa ketiga algoritma berdasarkan waktu pemrosesan, konsumsi sumber daya, keamanan hasil enkripsi dan efisiensi penyimpanan. Hasil evaluasi menunjukkan bahwa AES memiliki tingkat keamanan tinggi tetapi membutuhkan waktu pemrosesan lebih lama dibandingkan dengan Blowfish. DES menunjukkan kelemahan dalam aspek keamanan karena ukuran

Received Juli 31, 2025; Revised Agustus 28 , 2025;September 21, 2025
* Zefanya Seto Gandhara, zefanyaseto@gmail.com

kuncinya yang lebih kecil, sehingga lebih rentan terhadap serangan kriptografi. Blowfish menawarkan keseimbangan antara kecepatan pemrosesan dan keamanan, menjadikannya pilihan yang efisien untuk pengamanan video dengan performa yang lebih baik dibandingkan DES. Diharapkan dapat memberikan rekomendasi mengenai algoritma yang paling optimal untuk digunakan dalam pengamanan video digital baik dari segi efisiensi waktu, konsumsi sumber daya maupun tingkat keamanan.

Kata kunci: Kriptografi, AES, DES, Blowfish, Enkripsi Video.

LATAR BELAKANG

Dalam era digital yang semakin berkembang, keamanan data menjadi aspek krusial terutama dalam perlindungan terhadap informasi yang dikirim dan disimpan dalam bentuk video. Video digunakan secara luas dalam berbagai sektor mulai dari komunikasi, sistem pemantauan hingga layanan streaming (Adeniyi, Misra, Daniel, & Bokolo, 2022). Video juga menjadi sasaran utama serangan siber seperti penyadapan, manipulasi dan pencurian data. Dibutuhkan teknik kriptografi yang efektif untuk melindungi video dari akses yang tidak sah. Kriptografi merupakan metode pengamanan data yang digunakan untuk mengenkripsi dan mendekripsi informasi sehingga hanya pihak yang memiliki kunci tertentu yang dapat mengaksesnya. Beberapa algoritma kriptografi simetris yang umum digunakan dalam enkripsi video adalah Advanced Encryption Standard (AES), Data Encryption Standard (DES), dan Blowfish. Ketiga algoritma ini memiliki karakteristik dan tingkat keamanan yang berbeda yang dapat mempengaruhi efisiensi serta kecepatan pemrosesan data.

AES adalah standar enkripsi modern yang dikenal dengan tingkat keamanan tinggi dan efisiensi pemrosesan yang baik, menjadikannya pilihan utama dalam berbagai aplikasi keamanan data. DES meskipun menjadi standar sebelumnya memiliki kelemahan dalam ukuran kunci yang relatif kecil sehingga lebih rentan terhadap serangan brute force. Blowfish menawarkan fleksibilitas dalam ukuran kunci dan efisiensi yang lebih baik dibandingkan DES tetapi masih membutuhkan analisis lebih lanjut dalam penggunaannya untuk enkripsi video (Irawan & Rachmawanto, 2021). Penelitian ini bertujuan untuk mengevaluasi kinerja ketiga algoritma tersebut dalam pengamanan video dengan membandingkan aspek waktu pemrosesan, konsumsi sumber daya dan tingkat keamanan hasil enskripsi.

KAJIAN TEORITIS

Kriptografi dalam Pengamanan Data Video

Survei yang digunakan dalam penelitian ini berasal dari berbagai sumber akademik yang dapat diakses secara online Google Scholar. Sumber referensi ini dipilih karena menyediakan berbagai penelitian terdahulu mengenai kriptografi dan pengamanan video digital. Penulis juga mencari referensi dari penelitian terkait yang relevan dengan evaluasi algoritma AES, DES, dan Blowfish dalam konteks keamanan video.

1. Pemilihan Studi

a. Pencarian kata kunci, dilakukan sesuai dengan fokus penelitian ini dalam meninjau kinerja algoritma kriptografi dalam pengamanan video.

b. Eksplorasi dan pemilihan judul, abstrak serta kata kunci dilakukan berdasarkan kriteria kelayakan dimana hanya penelitian yang membahas enkripsi video dengan algoritma AES, DES dan Blowfish yang dipilih untuk ditinjau lebih lanjut.

c. Pembacaan lengkap atau sebagian penelitian dilakukan untuk menentukan apakah penelitian tersebut layak dimasukkan dalam tinjauan.

d. Daftar referensi dari setiap jurnal yang dipilih juga ditelaah untuk menemukan studi tambahan yang relevan dengan penelitian ini.

2. Pengumpulan Data

Pengumpulan data dilakukan secara manual dengan menggunakan alat bantu berupa tabel ekstraksi data. Tabel ini mencakup informasi seperti judul penelitian, nama penulis, tahun publikasi, nama jurnal/konferensi, jenis penelitian, topik utama, metode penelitian, hasil pembahasan, serta kesimpulan penelitian.

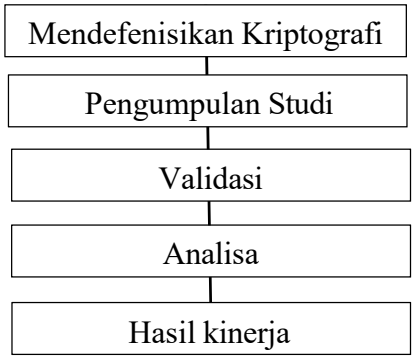
3. Pemilihan Item Data

Informasi yang diekstraksi dari setiap penelitian terdiri dari beberapa aspek utama, yaitu Evaluasi performa algoritma AES, DES, dan Blowfish dalam enkripsi video berdasarkan waktu pemrosesan dan konsumsi sumber daya. Analisis tingkat keamanan masing- masing algoritma dengan melihat efek avalanche dan sensitivitas perubahan kunci. Perbandingan efisiensi penyimpanan yang berfokus pada perubahan ukuran file

setelah proses enkripsidilakukan. Metode implementasi enkripsi video dan bagaimana setiap algoritma diterapkan dalam sistem keamanan digital.

METODE PENELITIAN

Terdapat beberapa langkah dalam penelitian ini yaitu dapat dilihat pada Gambar 1 dibawah ini:



Gambar 1 Metodologi Penelitian

HASIL DAN PEMBAHASAN

Seleksi Jurnal

Hasil pencarian dari berbagai database akademik seperti Google Scholar menghasilkan sejumlah studi yang membahas enkripsi video menggunakan algoritma AES, DES dan Blowfish. Dari hasil pencarian ini, ditemukan lima jurnal utama yang relevan dengan topik yang sedang dikaji. Jurnal-jurnal tersebut dipilih berdasarkan kelayakan dan keterkaitan dengan penelitian ini, dengan rentang publikasi dari tahun 2020 hingga 2024. Kriteria pemilihan jurnal mencakup aspek kesesuaian dengan enkripsi video, metode enkripsi yang digunakan, serta parameter evaluasi seperti waktu pemrosesan, keamanan, dan konsumsi sumber daya. Setelah seleksi dilakukan, kelima jurnal ini menjadi sumber utama untuk analisis dan komparasi dalam penelitian ini.

Karakteristik Jurnal

Informasi rinci dari kelima jurnal yang telah dipilih disajikan dalam Tabel 1 sebagai hasil dari ekstraksi data akhir. Ekstraksi ini hanya mencakup penelitian-penelitian yang memenuhi kriteria seleksi, termasuk jurnal yang membahas implementasi atau perbandingan algoritma AES, DES dan Blowfish dalam pengamanan video. Analisis dari jurnal-jurnal ini dilakukan untuk menilai efisiensi waktu pemrosesan, tingkat keamanan,

serta perbedaan utama dalam metode enkripsi yang diterapkan. Hasil dari tinjauan sistematis ini akan digunakan sebagai dasar dalam membandingkan kinerja masing-masing algoritma kriptografi dalam pengamanan video digital.

No	Penulis	Penelitian	Topik	Metode	Pembahasan	Kesimpulan	Perbedaan
1	Abidemi Emmanuel Adeniyi, Sanjay Misra, Eniola Daniel, Anthony Bokolo Jr.	Computational Complexity of Modified Blowfish Cryptographic Algoritmon Video Data	Meneliti performa algoritma Blowfish yang dimodifikasi untuk enkripsi video dengan fokus pada kompleksitas waktu eksekusi dan efek avalanche.	Membandingkan Blowfish standar dan Modified Blowfish dalam enkripsi video.	Blowfish standar memiliki tingkat keamanan lebih tinggi, dengan efek avalanche mencapai 50,71% dibandingkan Modified Blowfish 43,33%. Modified Blowfish lebih cepat dalam eksekusi dengan rata-rata waktu 248.4 ms dibandingkan 250.0 ms untuk Blowfish standar. Throughput Modified Blowfish lebih tinggi, Sehingga lebih efisien dalam enkripsi video.	Modified Blowfish lebih cepat dan memiliki throughput yang lebih tinggi, tetapi keamanan lebih rendah dibandingkan Blowfish standar.	Perbedaannya dengan penelitian ini terletak pada pendekatan yang digunakan. Jurnal ini berfokus pada pengembangan dan optimasi satu algoritma, sementara penelitian ini melakukan perbandingan langsung antara AES, DES, dan Blowfish dalam pengamanan video tanpa modifikasi struktur algoritma.
2	Candra Irawan, Eko Hari	Keamanan Data Menggunakan	Mengkaji kombinasi AES	Mengimplementasikan	AES-RSA memiliki efek avalanche tertinggi	Kombinasi AES dan RSA lebih aman	Perbedaannya dengan penelitian

	Rachmawanto	Gabungan Kriptografi AES dan RSA	dan RSA dalam proses enkripsi dan dekripsi berbagai	kombinasi AES-RSA dalam proses enkripsi dan dekripsi berbagai format file	(44,74%), lebih baik dibandingkan AES biasa. Waktu enkripsi meningkat seiring ukuran file yang lebih besar.Kombinasi AES dan RSA	daripada AES biasa, tetapi memerlukan waktu enkripsi yang lebih lama.	ini adalah fokusnya. Jurnal ini Mengevaluasi kombinasi dua algoritma, sementara penelitian ini membandingkan tiga algoritma

KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan penelitian ini dapatdisimpulkan bahwa AES, DES dan Blowfish memiliki keunggulan dan kelemahan masing-masing dalam pengamanan video digital. Algoritma AESterbukti efektif dalam menjaga keamanan data video, dengan tingkat keamanan yang tinggi dan kemampuan untuk mengenkripsi data secara efisien. Algoritma ini memiliki waktu enkripsi yang lebih lama dibandingkan dengan Blowfish. DES menunjukkan kelemahan dalam aspek keamanan karena ukuran kunci yang lebih kecil sehingga lebih rentan terhadap serangan brute force. Algoritma ini memiliki waktu eksekusi yang lebih cepat dibandingkan AES, tetapi tidak lagi dianggap aman untuk aplikasi enkripsi video modern. Blowfish memberikan keseimbangan antara keamanan dan efisiensi pemrosesan, dengan waktu enkripsi yang lebih cepat dibandingkan AES dan tingkat keamanan yang lebih baik dibandingkan DES. Ukuran kunci yang lebih fleksibel pada Blowfish membuat implementasinya lebih kompleks dibandingkan AES yang sudah memiliki standar tetap. Dari studi yang dilakukan dapat disimpulkan bahwa pemilihan algoritma tergantung pada kebutuhan spesifik dari aplikasi pengamanan video. Jika keamanan menjadi prioritas utama, AES merupakan pilihan terbaik karena tingkat keamanannya yang tinggi. Jika efisiensi waktu lebih diutamakan, Blowfish dapat menjadi alternatif karena proses enkripsinya yang lebih cepat. Sedangkan DES kurang direkomendasikan karena tingkat keamanannya yang lebih rendah dibandingkan dua algoritma lainnya. Sebagai tindak lanjut, penelitian di masa depan dapat mempertimbangkan kombinasi algoritma kriptografi untuk meningkatkan efisiensi

dan keamanan, serta menguji algoritma lain yang lebih baru dalam pengamanan video digital. Penelitian lebih lanjut dapat difokuskan pada optimasi enkripsi video dalam lingkungan sistem real-time seperti aplikasi streaming atau video conferencing, untuk melihat bagaimana algoritma ini bekerja dalam skenario yang lebih dinamis dan kompleks.

DAFTAR REFERENSI

Adeniyi, A. E., Misra, S., Daniel, E., & Bokolo, A. (2022). *Computational Complexity of Modified Blowfish Cryptographic Algorithm on Video Data. Algorithms*. *15*(373), 1–16.

Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA. *Proceeding SENDIU 2021*, 1–8.

Pratama, Y., & Sutabri, T. (2023). Analisis Kriptografi Algoritma Blowfish pada Keamanan Data Menggunakan Dart. Jurnal Teknologi Informasi dan Komputer, 10(2), 45-56.

Irawan, A. S. Y., El Ramdhani, A. F., Jordi, M., Mahdi, R. S., & Al Mudzakir, T. (2020). Pengamanan File Video dengan Algoritma Advanced Encryption Standard (AES). Systematics, 2(1), 28-32.

Kafa, N. A., & Sakti, D. V. S. Y. (2024). Implementasi Kriptografi Berbasis Web dengan Algoritma Advanced Encryption Standard (AES)

256 dan Kompresi Huffman untuk Pengamanan File di SMK Satria. Jurnal TICOM: Technology of Information and Communication, 12(2), 50-55.