LAPORAN PRAKTIKUM
PRAKTIK SISTEM KEAMANAN DATA

RESUME JURAL
AES (ADVANCED ENCRYTION STANDARD)

Disusun oleh :

Bimo Adji Kusnadi	(V3922010)
Catur Yudha Prasetya	(V3922011)
Fauzi Ihsan Anshori	(V3922021)
Fernando Dajak Satria	(V3922022)

Dosen
Yusuf Fadlila Rachman, S.Kom., M.Kom

PS D-III TEKNIK INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS SEBELAS MARET

2023

JURNAL 1	
Judul	Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit(Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)
Latar Belakang	Latar belakang masalah yang diangkat adalah pentingnya menjaga keamanan data dalam era digital, di mana pengiriman data melalui internet menjadi hal yang biasa dan masyarakat memiliki akses terhadap jaringan internet yang memadai.
Tujuan Penelitian	Penelitian ini bertujuan untuk merancang dan mengembangkan sebuah perangkat lunak keamanan informasi berbasis prototipe. Kami akan menggunakan metode Least Significant Bit (LSB) dan mengimplementasikan algoritma Advanced Encryption Standard (AES) dalam struktur perangkat lunak tersebut. Pendekatan ini dirancang untuk memastikan tingkat keamanan yang optimal, di mana LSB digunakan untuk menyisipkan informasi rahasia ke dalam bit-bit yang kurang signifikan, sementara AES akan bertanggung jawab atas enkripsi data secara menyeluruh. Selain proses pengembangan, penelitian ini juga akan fokus pada evaluasi sistem yang telah dikembangkan. Evaluasi ini akan mencakup uji keefektifan perangkat lunak dalam melindungi informasi, serta analisis tingkat keamanan terhadap potensi serangan. Dengan melakukan evaluasi menyeluruh, tujuan utama penelitian ini adalah untuk memastikan bahwa perangkat lunak pengamanan informasi yang dihasilkan tidak hanya efektif dalam menjaga kerahasiaan data tetapi juga mampu memberikan lapisan keamanan yang tinggi terhadap ancaman potensial.
Algoritma yang dipakai beserta alur penelitiannya	Metode penelitian ini melibatkan dua algoritma kunci, yakni metode Least Significant Bit (LSB) dan algoritma Advanced Encryption Standard (AES), dalam upaya untuk mengamankan informasi. Alur penelitian ini dirinci dalam beberapa tahapan sebagai berikut:Pengumpulan kebutuhan 1. Membangun prototyping 2. Evaluasi prototyping 3. Mengkodekan sistem 4. Menguji sistem 5. Evaluasi sistem 6. Menggunakan sistem

Hasil penelitian dan Kesimpulan	Hasil penelitian menunjukkan bahwa pengembangan perangkat lunak ini berhasil meningkatkan keamanan data dalam pengiriman melalui internet. Sistem yang dikembangkan telah diuji dan dievaluasi dengan baik, sehingga siap untuk diimplementasikan atau digunakan. Kesimpulannya, penggunaan metode LSB dan algoritma AES dalam pengembangan perangkat lunak pengamanan informasi dengan model prototype dapat meningkatkan keamanan data dalam pengiriman melalui internet.
Kelebihan dan kekurangan	Kelebihan jurnal ini adalah memberikan gambaran yang jelas dan terstruktur mengenai pengembangan perangkat lunak pengamanan informasi dengan model prototype menggunakan metode Least Significant Bit (LSB) dan algoritma Advanced Encryption Standard (AES). Selain itu, jurnal ini juga memberikan informasi mengenai spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam penelitian. Namun, kekurangan jurnal ini adalah tidak adanya penjelasan mengenai hasil uji coba yang lebih detail dan tidak adanya perbandingan dengan metode pengamanan informasi lainnya.

JURNAL 2	
Judul	Rancangan Aplikasi Pengamanan Data dengan Algoritma Advanced Encryption Standard (AES)
Latar Belakang	Latar belakang masalah yang diangkat dalam penelitian ini berkaitan dengan pesatnya perkembangan teknologi informasi dan komunikasi, terutama dalam pertukaran informasi melalui jaringan internet. Dalam konteks ini, kebutuhan akan keamanan data menjadi semakin krusial mengingat risiko dan ancaman terhadap kerahasiaan informasi yang dapat timbul seiring dengan kemajuan teknologi tersebut.
Tujuan Penelitian	Tujuan utama dari penelitian ini adalah merancang sebuah aplikasi pengamanan data yang mengimplementasikan algoritma Advanced Encryption Standard (AES). Dengan menerapkan algoritma ini, penelitian bertujuan untuk memastikan tingkat keamanan optimal terhadap data yang dipertukarkan melalui jaringan internet. Melalui aplikasi ini, diharapkan dapat memberikan lapisan keamanan yang kuat, mencegah akses tidak sah, dan menjaga kerahasiaan data yang terkirim. Dengan demikian, penelitian ini tidak hanya bertujuan untuk mengembangkan aplikasi yang efektif, tetapi juga untuk meningkatkan kepercayaan dalam pertukaran informasi digital di lingkungan online.
Algoritma yang dipakai beserta alur penelitiannya	Algoritma yang digunakan dalam penelitian ini adalah Advanced Encryption Standard (AES). Alur penelitiannya meliputi studi pustaka, analisis kebutuhan software, identifikasi permasalahan, desain algoritma pada kasus, implementasi, uji coba dan evaluasi, serta analisis hasil uji coba.
Hasil penelitian dan Kesimpulan	Hasil penelitian menunjukkan bahwa aplikasi pengamanan data yang dirancang dengan menggunakan algoritma AES dapat meningkatkan keamanan data yang dipertukarkan melalui jaringan internet. Dalam uji coba yang dilakukan, aplikasi ini mampu mengenkripsi dan mendeskripsi data dengan baik, serta dapat mengatasi masalah keamanan data yang sering terjadi. Kesimpulannya, penggunaan algoritma AES dalam aplikasi pengamanan data dapat meningkatkan keamanan data yang dipertukarkan melalui jaringan internet.

Kelebihan dan kekurangan	Kelebihan dari jurnal ini adalah penjelasan yang cukup lengkap tentang penggunaan algoritma AES dalam aplikasi pengamanan data, serta alur penelitian yang jelas dan sistematis. Namun, kekurangannya adalah kurangnya penjelasan tentang bagaimana aplikasi ini dapat diimplementasikan dalam kehidupan nyata, serta kurangnya penjelasan tentang kelemahan atau kekurangan dari penggunaan algoritma AES dalam aplikasi pengamanan data.