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	"Kriptografi dan Algoritma RSA"
Latar Belakang	Judul jurnal ini adalah "Kriptografi dan Algoritma RSA." Judul tersebut memberikan gambaran bahwa jurnal ini akan membahas tentang kriptografi secara umum dan fokus pada algoritma RSA. Latar belakang masalah dijelaskan dengan baik, dimulai dari perkembangan sistem informasi dan komunikasi yang meningkat pesat, terutama dalam pengiriman data melalui media non-kabel. Masalah integritas data dan kerahasiaan informasi muncul, dan kriptografi menjadi solusi untuk menjaga keamanan data tersebut.
Tujuan Penelitian	Tujuan penelitian tidak secara eksplisit disebutkan dalam jurnal. Meskipun demikian, tujuan umumnya dapat diidentifikasi sebagai pembahasan tentang kriptografi secara luas, dengan fokus khusus pada algoritma RSA. Tujuan penelitian sebaiknya dinyatakan secara jelas untuk memberikan pemahaman yang lebih baik kepada pembaca.
Algoritma yang dipakai beserta alur penelitiannya	Algoritma yang dibahas dalam jurnal ini adalah algoritma RSA. Penjelasan tentang algoritma ini cukup baik, dengan langkah-langkah pembangkitan pasangan kunci, enkripsi, dan dekripsi. Namun, beberapa bagian seperti perhitungan kunci dekripsi dan penggunaan rumus matematika bisa disederhanakan agar lebih mudah dipahami oleh pembaca yang tidak memiliki latar belakang matematika yang kuat.

Hasil penelitian	Penjelasan tentang aplikasi algoritma RSA pada tanda tangan digital memberikan tambahan informasi yang berguna. Namun, pembahasan ini dapat diperluas dengan memberikan contoh konkrit atau studi kasus yang memperkuat aplikasi algoritma tersebut..
Kelebihan dan kekurangan	Jurnal ini memberikan pemahaman yang baik tentang kriptografi dan algoritma RSA. Namun, beberapa bagian memerlukan penyederhanaan dan penjelasan tambahan. Penambahan contoh aplikasi algoritma RSA dapat memperkaya isi jurnal. Kesimpulannya, jurnal ini memberikan wawasan yang baik tentang topik yang dibahas, namun ada ruang untuk perbaikan dalam penyampaian informasi..

JURNAL 2	
Judul	"Studi Pemakaian Algoritma RSA dalam Proses Enkripsi dan Aplikasinya"
Latar Belakang	pemakaian algoritma RSA dalam proses enkripsi dan aplikasinya. Latar belakang masalahnya mencakup urgensi keamanan data dan kebutuhan untuk mengamankan pesan atau informasi yang dikirim melalui internet. Algoritma RSA dipilih karena dianggap sebagai salah satu algoritma enkripsi terkuat saat ini. Penelitian ini dilatarbelakangi oleh kebutuhan akan metode enkripsi yang efektif dan aman untuk melindungi data sensitif.
Tujuan Penelitian	Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem kriptografi dengan menggunakan algoritma RSA. Penelitian ini juga bertujuan untuk menguji kinerja sistem, memastikan bahwa aplikasi dapat berjalan dengan baik, dan memenuhi spesifikasi yang ditentukan.
Algoritma yang dipakai beserta alur penelitiannya	Penelitian ini mengikuti langkah-langkah klasik dari algoritma RSA, dimulai dari pemilihan dua bilangan prima, perhitungan parameter keamanan N, hingga pembentukan kunci publik dan kunci privat. Pemilihan bilangan bulat e, perhitungan d, dan proses pengujian sistem juga dijelaskan secara rinci. Implementasi sistem dilakukan dengan menggunakan bahasa pemrograman PHP dan web server Xampp.
Hasil penelitian dan Kesimpulan	Hasil penelitian mencakup implementasi perangkat lunak dengan algoritma RSA dan pengujian sistem. Sistem berhasil diuji untuk langkah-langkah enkripsi dan deskripsi, serta kunci publik dan privat berhasil dihasilkan. Kesimpulan dari penelitian ini menyatakan bahwa RSA merupakan algoritma enkripsi yang kuat, memiliki kunci publik dan privat, dan dapat digunakan untuk menyandikan data dengan aman. Kesimpulan ini didukung oleh hasil uji coba fitur-fitur yang menunjukkan bahwa aplikasi berjalan sesuai spesifikasi.

Kelebihan dan kekurangan	Jurnal ini memberikan wawasan yang baik tentang penggunaan algoritma RSA dalam konteks keamanan data. Dengan implementasi yang sukses dan pengujian yang memadai, jurnal ini memberikan kontribusi pada pemahaman praktis tentang penerapan algoritma kriptografi dalam pengembangan perangkat lunak. Referensi pustaka yang disertakan juga memperkuat dasar penelitian ini..