LAPORAN PRAKTIKUM
PRAKTIK SISTEM KEAMANAN DATA

RESUME JURAL
AES (ADVANCED ENCRYTION STANDARD)

Disusun oleh :

Rifqy Rivaldi	(V3922040)
Ody Frans Wijaya	(V3922037)
Sandy Aryasatya z	(V3922051)

Dosen

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

PS D-III TEKNIK INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS SEBELAS MARET
2023

JURNAL 1	
Judul	"Studi Pemakaian Algoritma RSA dalam Proses Enkripsi dan Aplikasinya"
Latar Belakang	Penggunaan algoritma RSA dalam proses enkripsi dan implementasinya. Permasalahan tersebut dilatarbelakangi oleh mendesaknya keamanan informasi dan perlunya perlindungan terhadap pesan atau informasi yang dikirim melalui Internet. Algoritma RSA dipilih karena dianggap sebagai salah satu algoritma enkripsi terkuat yang ada saat ini. Penelitian ini dilatarbelakangi oleh perlunya metode enkripsi yang efektif dan aman untuk melindungi data sensitif..
Tujuan Penelitian	Tujuan dari penelitian ini adalah untuk mengimplementasikan sistem enkripsi menggunakan algoritma RSA. Tujuan dari penelitian ini juga untuk menguji kinerja sistem, untuk memastikan bahwa aplikasi bekerja dengan baik danmemenuhi persyaratan yang ditentukan.
Algoritma yang dipakai beserta alur penelitiannya	Penelitian ini mengikuti langkah-langkah klasik algoritma RSA, dimulai dari memilih dua bilangan prima, menghitung parameter keamanan N, dan menghasilkan kunci publik dan kunci privat. Dijelaskan juga secara rinci pemilihan bilangan bulat e, perhitungan d, dan proses pengujian sistem. Sistem diimplementasikan menggunakan bahasa pemrograman PHP dan web server Xampp.
Hasil penelitian dan Kesimpulan	Hasil penelitian meliputi implementasi perangkat lunak dengan algoritma RSA dan pengujian sistem. Fase enkripsi dan deskripsi sistem berhasil diuji dan kunci publik dan privat berhasil dihasilkan. Temuan penelitian ini menunjukkan bahwa RSA merupakan algoritma kriptografi kunci publik-pribadi yang kuat dan dapat digunakan untuk mengenkripsi data dengan aman. Kesimpulan ini didukung oleh hasil pengujian fungsi yang menunjukkan bahwa aplikasiberfungsi sesuai yang ditentukan.
Kelebihan dan kekurangan	Kelebihan dan Kekurangan Artikel ini memberikan gambaran yang baik tentang penggunaan algoritma RSA dalam konteks keamanan informasi. Melalui implementasi yang sukses dan pengujian yang memadai, artikel ini berkontribusi pada pemahaman praktis tentang penerapan algoritma kriptografi dalam perangkat lunak. Landasan penelitianini juga diperkuat dengan referensi literatur yang menyertainya..

JURNAL 2	
Judul	"Kriptografi dan Algoritma RSA"
Latar Belakang	Jurnal ini disebut "Kriptografi dan Algoritma RSA". Judulnya menunjukkan bahwa artikel ini membahas tentang kriptografi secara umum dan berfokus pada algoritma RSA. Latar belakang permasalahan tersebut dapat dijelaskan dengan baik, dimulai dari semakin pesatnya perkembangan sistem informasi dan komunikasi, khususnya dalam transmisi data melalui media non-kabel. Masalah integritas dan kerahasiaan data muncul, dan kriptografi menjadi solusi untuk menjaga keamanan data tersebut.
Tujuan Penelitian	Tujuan penelitian tidak disebutkan secara langsung dalam jurnal. Namun, diskusi luas tentang enkripsi, khususnya algoritma RSA, dapat didefinisikan sebagai tujuan umum. Tujuan makalah penelitian harus dinyatakan dengan jelas agar pembaca dapat lebih memahaminya.
Algoritma yang dipakai beserta alur penelitiannya	Algoritma yang dibahas pada artikel ini adalah algoritma RSA. Penjelasan algoritma ini cukup baik, dengan langkah-langkah untuk menghasilkan, mengenkripsi dan mendekripsi pasangan kunci. Namun, beberapa bagian, seperti penghitungan kunci dekripsi dan penggunaan rumus matematika, dapat disederhanakan agar lebih mudah dipahami oleh pembaca yang tidak memiliki latar belakang matematika yang kuat..
Hasil penelitian dan Kesimpulan	Penjelasan penerapan algoritma RSA untuk tanda tangan digital memberikan informasi tambahan yang berguna. Namun pembahasan ini dapat diperluas dengan memberikan contoh spesifik atau studi kasus yang memperkuat penerapan algoritma.

Kelebihan dan kekurangan	Jurnal ini memberikan gambaran yang baik tentang kriptografi dan algoritma RSA. Namun, beberapa poin memerlukan penyederhanaan dan penjelasan lebih lanjut. Menambahkan contoh penerapan algoritma RSA dapat memperkaya konten majalah. Singkatnya, dapat dikatakan bahwa majalah ini menawarkan pemahaman yang baik tentang topik yang dibahas, namun masih ada ruang untuk perbaikan dalam penyampaian informasi..