

A. REVIEW JURNAL

Judul	"Kriptosistem Hybrid Menggunakan Kombinasi AES dan RSA untuk Enkripsi Teks Pesan".
Nama Jurnal	JOCOTIS - Journal Science Informatica and Robotics
Volume & Halaman	Volume 1 Nomor 1 September 2023 Hal. 22-31
Tahun	2023
Penulis	Steven Richardo Siburian, Sultan P, Riski Alek Syaputra Sinaga, dan Fikri Yudistira.
Reviewer	Audrey Surya N (V3922008) Diah Munica N (V3922015) Fabianus Jan Krisna W (V3922017)
Tanggal	11 November 2023

Latar Belakang Masalah	Artikel ilmiah ini dibuat untuk menyelesaikan tugas mata kuliah Keamanan Perangkat Lunak. Artikel ilmiah ini dilaksanakan untuk memberikan pemahaman tentang betapa pentingnya menjaga keamanan informasi yang ada di dalam pesan teks. Dalam penggunaan teks pesan yang ada pada saat ini, terdapat kurangnya tingkat keamanan yang dapat mengancam privasi dan kerahasiaan data informasi yang dikirim. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan Kriptosistem Hybrid yang lebih aman dengan mengkombinasikan algoritma AES dan RSA.
Tujuan Penelitian	Tujuan dari penelitian ini adalah untuk mengembangkan Kriptosistem Hybrid yang lebih aman dengan mengkombinasikan algoritma AES dan RSA untuk meningkatkan keamanan pada Teks Pesan.
Algoritma dan Alur Penelitian	Penelitian ini menggunakan metode Studi Literatur untuk merangkum dan menganalisis sumber-sumber terpercaya dan valid tentang penggunaan Kriptosistem Hybrid dengan menggunakan kombinasi AES dan RSA untuk meningkatkan keamanan pada Teks Pesan. Penelitian ini juga membahas tentang algoritma AES dan RSA serta cara mengimplementasikan kriptosistem hybrid pada aplikasi pesan teks.

<p>Hasil Penelitian dan Kesimpulan</p>	<p>Hasil Penelitian dan Kesimpulan: Hasil dari penelitian ini adalah pengembangan Kriptosistem Hybrid yang lebih aman dengan mengkombinasikan algoritma AES dan RSA yang dapat mengenkripsikan teks pesan sehingga dapat meningkatkan keamanan yang lebih ketat untuk melindungi privasi dan kerahasiaan data informasi yang dikirim. Dalam kesimpulannya, penelitian ini menunjukkan bahwa penggunaan kombinasi AES dan RSA dalam enkripsi teks pesan dapat meningkatkan keamanan dan privasi data informasi yang dikirim. Selain itu, penelitian ini juga menunjukkan bahwa algoritma AES dan RSA telah banyak diterapkan dalam mengatasi masalah keamanan data, dan penggunaan kombinasi keduanya dalam Kriptosistem Hybrid diharapkan dapat meningkatkan keamanan dan melindungi privasi serta kerahasiaan informasi yang dikirimkan. Namun, penelitian ini juga mengakui bahwa penggunaan Kriptosistem Hybrid dapat memakan waktu dan sumber daya yang lebih banyak dibandingkan dengan penggunaan enkripsi tunggal. Oleh karena itu, perlu dilakukan evaluasi dan pengujian lebih lanjut untuk menentukan apakah penggunaan Kriptosistem Hybrid ini layak digunakan dalam aplikasi chat yang lebih besar dan kompleks.</p>
<p>Kelebihan dan Kekurangan</p>	<p><i>Kelebihan:</i></p> <ul style="list-style-type: none"> - Meningkatkan keamanan dan privasi data informasi yang dikirimkan. - Kombinasi AES dan RSA telah banyak diterapkan dalam mengatasi masalah keamanan data. - Hanya pemegang kunci privat yang dapat mengakses dan mendekripsi pesan yang dikirimkan. - Kriptosistem Hybrid dapat memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan penggunaan enkripsi tunggal. <p><i>Kekurangan:</i></p> <ul style="list-style-type: none"> - Penggunaan Kriptosistem Hybrid dapat memakan waktu dan sumber daya yang lebih banyak dibandingkan dengan penggunaan enkripsi tunggal. - Perlu dilakukan evaluasi dan pengujian lebih lanjut untuk menentukan apakah penggunaan Kriptosistem Hybrid ini layak digunakan dalam aplikasi chat yang lebih besar dan kompleks. - Kriptosistem Hybrid memerlukan penggunaan dua jenis algoritma enkripsi yang berbeda, sehingga memerlukan pengetahuan dan keterampilan yang lebih tinggi untuk mengimplementasikannya.