

BAB IV

SIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang dilakukan enkripsi dan dekripsi gambar menggunakan algoritma RSA serta teknik pengacakan dengan *Cesar cipher* dan permutasi, dapat diambil kesimpulan sebagai berikut: (i) Teknik *scrambling* yang melibatkan *Cesar cipher* dan permutasi berhasil meningkatkan kerandoman gambar, seperti yang ditunjukkan oleh peningkatan entropi setelah proses *scrambling*. *Cesar cipher* menggeser nilai-nilai piksel berdasarkan posisi piksel, sementara permutasi menukar baris dan kolom gambar secara acak, menghasilkan gambar yang sulit dikenali tanpa kunci yang tepat. (ii) Algoritma RSA berhasil mengenkripsi gambar yang telah di-*scrambling*, menghasilkan data terenkripsi dengan entropi yang sangat tinggi, mencerminkan kerandoman maksimum. Proses dekripsi dengan kunci privat RSA berhasil mengembalikan gambar ke bentuk *scrambled* sebelum enkripsi, yang kemudian dapat di-*unscramble* kembali ke bentuk aslinya dengan benar. (iii) Proses enkripsi dan *scrambling* yang diterapkan memberikan tingkat keamanan yang baik untuk data gambar, menjadikannya sulit dikenali dan diakses tanpa kunci yang tepat. Penggunaan entropi sebagai ukuran kerandoman efektif dalam menganalisis perubahan yang terjadi pada gambar selama proses enkripsi dan dekripsi.

4.2 Saran

Berdasarkan hasil analisis ini, beberapa saran dapat diberikan untuk pengembangan lebih lanjut: (i) Mengingat algoritma RSA memiliki keterbatasan dalam ukuran data yang dapat dienkripsi sekaligus, disarankan untuk mengeksplorasi metode enkripsi yang lebih efisien untuk gambar yang berukuran besar, seperti kombinasi RSA dan AES (*Advanced Encryption Standard*). (ii) Peningkatan keamanan kunci menggunakan kunci yang lebih panjang dan kompleks dalam algoritma RSA dapat meningkatkan keamanan lebih lanjut terhadap serangan kriptografi. Hal ini dapat dilakukan dengan memperluas rentang nilai untuk p dan q dalam generasi kunci RSA. (iii) Integrasi teknik ini dengan sistem keamanan yang lebih luas, seperti sistem autentikasi dan otorisasi yang kuat, akan memberikan perlindungan tambahan terhadap akses tidak sah. (iv) Penelitian lebih lanjut dapat dilakukan untuk mengoptimalkan performa enkripsi dan dekripsi, terutama untuk gambar dengan resolusi tinggi atau dalam skala besar. (v) Uji cobalah pada berbagai jenis gambar dan format yang berbeda akan membantu dalam memahami lebih baik keandalan dan fleksibilitas metode ini dalam berbagai skenario. Dengan saran-saran ini, diharapkan teknik pengacakan dan enkripsi gambar dapat lebih disempurnakan dan diimplementasikan secara efektif dalam praktik keamanan digital. (vi) Studi khusus lebih lanjut dengan menggunakan gambar yang lebih besar dan beragam, untuk mengevaluasi kinerja dan keamanan dari pendekatan yang diusulkan. Untuk peneliti kedepannya bisa lebih teliti lagi untuk menreapkan algoritma RSA dalam enkripsi dan dekripsi pada citra digital.