BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan secara sistematis mengenai *"Implementasi Algoritma Kriptografi AES-256 untuk Keamanan Data pada Sistem Ujian Berbasis Web"*, maka dapat dirumuskan sejumlah simpulan sebagai berikut:

1. Penulis berhasil merancang dan membangun sistem ujian berbasis web dengan keamanan data menggunakan algoritma kriptografi AES-256 di sisi *frontend*. Sistem dikembangkan dengan JavaScript menggunakan NextJs untuk *frontend*, Express.js untuk *backend*, serta MySQL sebagai basis data. Proses pengembangan mengacu pada rancangan diagram UML, *wireframe*, ERD, serta flowchart enkripsi dan dekripsi.
2. Hasil pengujian Wireshark menunjukkan data sensitif berhasil terenkripsi selama transmisi, terlihat dari ciphertext pada packet capture, sedangkan uji Black box membuktikan seluruh fitur utama seperti enkripsi–dekripsi, autentikasi, dan manajemen ujian berjalan baik tanpa error.
3. Analisis Korelasi Pearson terhadap data plaintext dan ciphertext menghasilkan nilai mendekati nol, yang mengindikasikan tidak adanya hubungan linier antara keduanya. Hal ini membuktikan efektivitas enkripsi AES-256 dalam menjaga kerahasiaan data dan menunjukkan kualitas enkripsi yang tinggi.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut adalah sebagai berikut:

1. Meskipun algoritma AES-256 sudah berjalan dengan baik, pengoptimalan pada sisi *frontend* maupun *backend* dapat dilakukan untuk meningkatkan kecepatan dan efisiensi, khususnya pada perangkat dengan spesifikasi rendah.

2. Skema enkripsi sebaiknya tidak terbatas hanya pada data berbentuk teks, tetapi juga mencakup format data lainnya. Selain itu, perlu dilakukan pengujian keamanan terhadap implementasi algoritma kriptografi AES-256 di sisi aplikasi web, seperti uji ketahanan terhadap serangan *Man-in-the-Middle* maupun *Brute Force attack*, guna memastikan sistem benar-benar aman.
3. Penelitian selanjutnya dapat melakukan uji coba pada jumlah pengguna dan volume data yang lebih besar untuk mengevaluasi kestabilan dan performa sistem dalam skenario penggunaan berskala besar.