BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilaksanakan mengenai implementasi kriptografi pada database berbasis web dengan menggunakan algoritma Advanced Encryption Standard (AES), dapat disimpulkan bahwa penerapan algoritma AES secara efektif mampu meningkatkan tingkat keamanan data yang tersimpan dalam database. Proses enkripsi yang diterapkan berfungsi untuk mengubah data asli (plaintext) menjadi data yang teracak (ciphertext), sehingga informasi yang disimpan tidak dapat diakses atau dibaca oleh pihak yang tidak memiliki otoritas atau kunci dekripsi. Dengan demikian, meskipun terjadi upaya akses ilegal terhadap database, kerahasiaan data tetap terjaga dengan baik.

Implementasi algoritma AES pada sistem yang dirancang menunjukkan bahwa proses enkripsi dan dekripsi berjalan sesuai dengan rancangan. Data berhasil dienkripsi sebelum disimpan di dalam database dan dapat didekripsi kembali dengan baik saat diakses oleh pengguna yang memiliki hak akses. Hasil uji coba sistem juga memperlihatkan bahwa seluruh fungsi berjalan sesuai kebutuhan, mulai dari proses penyimpanan, enkripsi, dekripsi data, hingga autentikasi pengguna.

Selain memberikan jaminan keamanan, penggunaan algoritma AES juga terbukti efisien dalam hal kecepatan proses enkripsi dan dekripsi tanpa mengorbankan tingkat keamanan. Dengan panjang kunci sebesar 256-bit, algoritma AES memiliki tingkat perlindungan yang tinggi sehingga sangat direkomendasikan untuk mengamankan data sensitif dalam sistem basis data berbasis web.

5.2 Saran

Berdasarkan temuan dalam penelitian ini, terdapat beberapa rekomendasi untuk pengembangan sistem lebih lanjut di masa mendatang. Salah satunya adalah peningkatan sistem keamanan dengan menambahkan fitur manajemen kunci yang lebih optimal, seperti implementasi protokol pertukaran kunci secara aman atau penerapan skema kriptografi hibrida yang menggabungkan algoritma kriptografi

simetris (AES) dengan algoritma kriptografi asimetris, seperti RSA, untuk meningkatkan keamanan dalam proses distribusi kunci.

Selain itu, untuk mendukung integritas data serta proses autentikasi pengguna, disarankan penerapan fungsi hashing dengan algoritma yang kuat, misalnya SHA-256, guna memastikan data tidak mengalami perubahan selama proses penyimpanan atau transmisi. Pengembangan lanjutan juga dapat diarahkan pada peningkatan keamanan komunikasi antara aplikasi dengan database melalui penerapan protokol SSL/TLS, sehingga dapat mencegah potensi intersepsi atau pencurian data selama proses transmisi.