BAB V
PENUTUP

5.1 Kesimpulan

AES menawarkan keamanan yang lebih tinggi dengan dukungan untuk panjang kunci yang lebih besar (128-bit, 192-bit, 256-bit), sementara DES terbatas pada panjang kunci 56-bit.Panjang kunci yang lebih besar pada AES membuatnya lebih tahan terhadap serangan brute-force modern, sementara panjang kunci yang terbatas pada DES meningkatkan risiko keamanan. Mode operasi enkripsi, seperti ECB, CBC, CFB, OFB, dan CTR, dapat mempengaruhi keamanan informasi. CBC dan CTR seringkali lebih disarankan untuk meningkatkan keamanan dibandingkan ECB pada implementasi praktis.

5.2 Saran

Jika masih ada implementasi yang menggunakan DES, disarankan untuk segera mempertimbangkan migrasi ke AES. AES menawarkan tingkat keamanan yang lebih tinggi dan memiliki ketersediaan dukungan yang lebih baik.Pendidikan dan kesadaran pengguna tentang pentingnya keamanan informasi dan pemilihan algoritma enkripsi yang tepat juga merupakan faktor kunci. Pengguna dan pengembang perlu memahami praktik terbaik dan potensi risiko terkait dengan penggunaan algoritma tertentu.