Bab V
Kesimpulan

Kemajuan teknologi informasi yang pesat telah menciptakan kebutuhan yang mendesak akan sistem keamanan yang kuat untuk melindungi data sensitif, terutama dalam jaringan yang saling berhubungan. Banyak aplikasi perpesanan yang tersedia saat ini masih kekurangan langkah-langkah keamanan yang memadai, sehingga membuat privasi pengguna rentan terhadap akses tidak sah dan ancaman kejahatan dunia maya. Untuk mengatasi masalah ini, diusulkan pengembangan sebuah aplikasi perpesanan yang aman dengan mengimplementasikan algoritma *Advanced Encryption Standard (AES)* serta *Secure Hash Algorithm 256 (SHA-256)* untuk melakukan enkripsi dan dekripsi. Tujuannya adalah untuk memastikan privasi dan keamanan data pengguna dalam proses pengiriman pesan.

Penelitian ini berfokus pada penggabungan algoritma AES dan SHA-256 dalam meningkatkan keamanan kata sandi dan pesan dalam sebuah aplikasi obrolan berbasis web. Penelitian ini akan mengevaluasi durasi yang diperlukan untuk proses enkripsi dan dekripsi, serta menguji Efek Longsoran, yang merupakan pengukuran perubahan dalam *ciphertext* saat ada perubahan kecil pada *plaintext*. Melalui pendekatan ini, penelitian ini bertujuan untuk mengatasi kekurangan keamanan yang ada dalam aplikasi perpesanan dengan mengimplementasikan teknik kriptografi yang lebih canggih.

Kriptografi adalah seni dan ilmu mengubah teks asli (*plaintext*) menjadi teks terenkripsi (*ciphertext*) untuk melindungi informasi dari akses yang tidak sah. Proses ini melibatkan dua fungsi utama: enkripsi (mengalihkan plaintext menjadi ciphertext) dan dekripsi (mengembalikan *ciphertext* menjadi *plaintext*). Fungsi hash adalah metode kriptografi yang mengubah input dengan panjang variabel menjadi output dengan panjang tetap. Fungsi ini memberikan transformasi satu arah yang sangat sulit untuk dibalik. Algoritma SHA-256, menghasilkan hash sepanjang 256-bit dan dirancang untuk tahan terhadap tabrakan, dimana dua input berbeda menghasilkan hash yang sama. Proses padding dalam SHA-256 dan pentingnya menjaga integritas data selama transmisi juga dijelaskan dalam konteks bagaimana SHA-256 dapat memastikan bahwa data tidak diubah selama pengiriman.

Efek Longsoran adalah fenomena dalam kriptografi di mana perubahan kecil pada plaintext menyebabkan perubahan besar pada ciphertext. Dalam konteks keamanan enkripsi, algoritma yang baik harus menunjukkan perubahan signifikan, biasanya antara 45% hingga 60%, dalam ciphertext ketika plaintext sedikit dimodifikasi. Hal ini membuat tidak gampang bagi penyerang untuk mendekripsi atau menebak teks asli.

Data yang digunakan dalam penelitian ini meliputi hasil dari implementasi algoritma enkripsi dan dekripsi, waktu rata-rata yang dibutuhkan untuk melindungi akun, serta pengujian Efek Longsoran. Analisis ini bertujuan untuk menilai tingkat efektivitas kombinasi algoritma AES dan SHA-256 dalam melindungi pesan pengguna selama transmisi, serta mengukur kinerja dan keamanan sistem yang diusulkan. Desain aplikasi yang diusulkan mengintegrasikan algoritma AES dan SHA-256 untuk mengamankan kata sandi pengguna selama proses pendaftaran akun dan pengiriman pesan. Proses enkripsi dalam aplikasi ini mencakup langkah-langkah seperti hashing, operasi XOR, dan pembuatan Vektor Inisialisasi acak (IV) untuk memastikan keamanan data. Tujuan dari desain ini adalah untuk menciptakan aplikasi perpesanan yang aman di mana kunci enkripsi tidak disimpan langsung di dalam database, sehingga mengurangi risiko akses tidak sah.

Hasil penelitian menunjukkan bahwa kombinasi algoritma AES dan SHA-256 secara signifikan mampu meningkatkan privasi dan keamanan data pengguna. AES, sebagai algoritma enkripsi simetris, menawarkan tingkat keamanan yang tinggi dengan kunci enkripsi yang kuat dan proses enkripsi yang efisien. Di sisi lain, SHA-256, sebagai algoritma hash kriptografis, memastikan integritas data dengan menghasilkan hash yang unik dan tahan terhadap tabrakan, sehingga setiap perubahan kecil pada data input akan menghasilkan hash yang sangat berbeda. Penggunaan kedua algoritma ini secara bersamaan menciptakan lapisan keamanan ganda yang efektif dalam melindungi informasi pengguna dari berbagai ancaman, seperti pencurian data atau akses tidak sah. Hasil penelitian juga menunjukkan bahwa sistem yang diusulkan mampu menghasilkan Efek Longsoran dalam kisaran yang diharapkan, yaitu antara 45% hingga 60%. Hal ini berarti bahwa setiap modifikasi kecil pada pesan asli menyebabkan perubahan yang cukup besar pada pesan terenkripsi, sehingga meningkatkan kesulitan bagi penyerang untuk menebak atau mendekripsi pesan asli.