BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan hasil dari pengujian serta analisis penerapan algoritma *Advanced Encryption Standard* (AES-256) dengan mode *Chiper Block Chaining* (CBC) dan *Secure Hash Algorithm* (SHA-256) terhadap aplikasi yang telah dibuat yaitu aplikasi enkripsi dan dekripsi file berbasis Windows yaitu *Secret Fichier*. Dapat disimpulkan beberapa point sebagai berikut :

a. Untuk Mencegah terjadinya kebocoran data yang bersifat penting dan merugikan beberapa pihak, oleh karena itu data bersifat penting harus di enkripsi terlebih dahulu dengan aplikasi *Secret Fichier* untuk melindungi data penting pada Univeristas Bhayangkara Jakarta Raya.
b. Aplikasi *Secret Fichier* mampu mengenkripsi file dengan berbagai ekstensi seperti file dokumen, file suara (voice note/mp3), file video serta file gambar dengan baik dan dapat didekripsikan kembali dengan kunci yang sama pada aplikasi *Secret Fichier*, aplikasi ini mampu mengamankan data bersifat penting untuk Universitas Bhayangkara Jakarta Raya sebagai penerapan baku dari aplikasi enkripsi berbasis dekstop.
c. Algoritma AES mode CBC dan SHA yang diterapkan di aplikasi dapat berjalan dengan baik tanpa kendala di aplikasi Secret Fichier untuk mengenkripsi file dan mendekripsikan nya di dalam sistem operasi Windows 10 64 bit.
d. Algoritma AES dan SHA dapat dibilang masih cukup aman didalam pemprosesannya dikarenakan mempunyai kunci yang panjang dan tahapan perhitungan yang cukup rumit di dalamnya.
e. Pada proses pengenkripsian file terdapat perbedaan ukuran file asli dengan file yang dienkripsi dikarenkan adanya proses *padding* didalam proses pengenkripsian tersebut, sehingga menunjukan perbedaan ukuran file asli dengan file yang telah di enkripsi.

5.2 Saran

Untuk penelitian lebih lanjut, perlu dipertimbangkan kembali berdasarkan kesimpulan yang telah dipaparkan diatas. berikut untuk saran saran untuk penelitian selanjutnya :

a. Untuk penelitian selanjutnya, disarankan untuk dapat mengenkripsi file dengan berukuran lebih besar dan dapat dijalan di sistem operasi lainnya (tidak hanyak windows).
b. Untuk penelitian selanjutnya, pertimbangkan kembali untuk menggunakan mode operasi yang lainnya, seperti CFB (Chiper FeedBack), OFB (Output FeedBack) atau GCM (Galois Counter Mode).
c. Untuk penelitian selanjutnya, disarankan untuk dapat menggunakan seri SHA terbarukan yaitu SHA-3.
d. Untuk penelitian selanjutnya, pertimbangkan kembali untuk menggunakan algoritma asimetris. Dimana memiliki dua kunci yang berbeda untuk keamanannya.
e. Untuk penelitian selanjutnya, aplikasi *Secret Fichier* dapat dikembangkan dan diterapkan pada *mobile* atau menjadi sebuah fitur *independent* dalam sebuah aplikasi *messenger*.
f. Penerapan Electronic Data Interchange (EDI) bisa menjadi salah satu solusi untuk membuat keamanan dalam transaksi bisnis di Internet dan dalam pertukaran file melalui handshakes file.