

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil dari analisis, pembahasan dan serangkaian pengujian yang telah dilakukan terhadap aplikasi AES Crypto-D menggunakan algoritma *Advanced Encryption Standard* (AES) ini, diambil kesimpulan bahwa aplikasi ini sudah berjalan dengan benar sesuai konsep serta rumusan masalah yang sudah dibuat sebelumnya, yaitu dengan menerapkan algoritma Rijndael yang terdiri dari 4 jenis transformasi bytes, yang terdiri dari: SubBytes, ShiftRows, MixColumns, dan AddRoundKey.

Dari ke-4 transformasi tersebut, dalam setiap putaran algoritma Rijndael memiliki panjang kunci yang berbeda-beda seperti : 128, 192, dan 256 bit. Yang nantinya dari masing-masing *key size* tersebut memiliki jumlah putaran transformasi yang berbeda sesuai dengan jumlah bit-nya.

5.2 Saran

Program aplikasi AES Crypto-D ini tidak jauh berbeda dengan aplikasi lain pada umumnya yang masih memiliki banyak kekurangan, dan diharapkan kedepannya agar program ini dapat dikembangkan lebih lanjut, karena dalam implementasi aplikasi ini hanya dalam cakupan kecil dan sangat mendasar yang hanya dengan menggunakan Microsoft Visual Basic 6.0. Saran bagi penelitian selanjutnya, yaitu mengkombinasikan algoritma yang ada dengan algoritma yang lain sehingga aplikasi ini dapat memberikan proteksi yang lebih maksimal. Dan semoga penelitian selanjutnya bisa dibuat pada model smartphone berbasis android, karna untuk kedepannya nanti topik tentang android masih bagus untuk dikembangkan.

