BAB V

KESIMPULAN

Kesimpulan yang didapatkan dari "ANALISIS KOMPARATIF KEAMANAN DATA MENGGUNAKAN ALGORTMA *MD5*, *SHA256*, *AES*, TERHADAP KINERJA SERVER" adalah sebagai berikut:

1. Dari hasil pengujian skenario dengan besarnya data dengan jenis file yang berbeda-beda, algoritma enkripsi yang paling optimal adalah *MD5*. Dikarenakan MD5 hanya membutuhkan waktu 38 milidetik untuk memproses data sebesar 20 MB, sedangkan SHA256 dan AES membutuhkan waktu di atas 100 milidetik. Dan MD5 membutuhkan CPU sebesar 3%, sedangkan SHA256 sebesar 9% dan AES sebesar 52%. Perubahan Besar data yang dienkripsi tidak mempengaruhi pemakaian RAM.
2. Hasil tes dari skenario kedua enkripsi data yang banyak sekaligus dengan panjang pesan 10 karakter, algoritma *MD5* lebih optimal dibandingkan dengan algoritma yang lainnya. MD5 menggunakan CPU sebesar 28% untuk mengenkripsi data yang banyak sekaligus, sedangkan SHA256 mengunakan CPU sebesar 55% dan AES sebesar 42%.
3. Algoritma *AES* lebih unggul dibandingkan dengan algoritma *MD5* dan *SHA256*. Dikarenakan algoritma *AES* menggunakan secretkey dan bisa dideskripsikan kembali sedangkan algoritma *SHA256*, dan *MD5* tidak bisa dekripsikan kembali. Sehingga untuk mengetahui pesan awal yang dienkripsi yang dilakukan adalah dengan mencocokan data awal dan nilai hash.