BAB V Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat ditarik kesimpulan bahwa:

1. Setelah dilakukan penelitian mendalam dengan menggunakan *framework* lainnya, dapat disimpulkan bahwa Laravel merupakan framework yang tepat untuk penelitian ini, dimana *package* bernama FileVault dapat digunakan untuk mengenkripsi dan dekripsi *file* tipe .docx dan .pdf menggunakan AES.
2. Dengan studi literatur dan percobaan sistem lainnya, penulis menyimpulkan bahwa pengamanan *secret key* dapat dilakukan dengan cara menyimpan hasil *hash* menggunakan Bcrypt didalam *database* dengan memanfaatkan fitur Hash.
3. Komputer 1 unggul dalam lama waktu pemrosesan algoritma AES dari komputer 2, dengan enkripsi docx memiliki perbedaan sebesar 0.406%, lalu dekripsi docx dengan nilai 72,571% dan dekripsi pdf dengan 48,254%. Komputer 2 hanya unggul pada waktu enkripsi pdf dengan perbedaan waktu sebesar 41,649%.
4. Saat *file* dienkripsi terdapat penambahan pada ukuran *file*. Perbedaan ukuran file docx komputer 1 dan 2 antara besar asli dan besar file terenkripsi serta besar file terenkripsi dengan besar file terdekripsi yaitu sebesar 0,396%. Sedangkan pada file pdf memiliki nilai 0,393%. Hal ini menunjukkan bahwa ukuran *file* meningkat dan menurun dengan kecil dan stabil.
5. Semakin besar ronde pada Bcrypt yang diinputkan, maka akan semakin lama waktu yang dibutuhkan untuk melakukan *hashing* pada suatu teks. Kenaikan waktunya untuk setiap pergantian ronde bervariasi dari 22,788% hingga 57,765%.

6. Waktu yang dibutuhkan untuk *hashing* kunci lebih besar daripada saat proses cek kunci atau *secret key*, dengan rincian komputer 1 untuk pdf dan docx yaitu 0,636% dan 4,087%, sedangkan pada komputer 2 pada pdf dan docx memiliki nilai 2,818% dan 0,988% .
7. Perbedaan waktu untuk *hashing secret key* pdf antara komputer 1 dan 2 dimana komputer 2 lebih cepat yaitu sebesar 17,261%, untuk cek *secret key* pdf sebesar 15,467%, sedangkan untuk *hashing secret key* docx sebesar 17,143% dan cek *secret key* mendapatkan nilai sebesar 19,611%.
8. Kombinasi teks *secret key* tidak berpengaruh dalam lama enkripsi dan dekripsi dari *file* pdf dan docx.Meskipun begitu, sangat disarankan untuk selalu menggunakan kunci yang tidak mudah ditebak dan dipecahkan.
9. File yang di enkripsi menggunakan AES mempunyai nilai *hash* yang berbeda.
10. Hasil *hashing* dari Bcrypt menunjukkan teknik *hash* yang dilakukan dapat menghasilkan teks yang lebih sedikit dari teks originalnya, dengan panjang heksadesimal yang konsisten yaitu 24 karakter.

5.2 Saran

Untuk penelitian yang akan datang, disarankan untuk:

1. Menggunakan algoritma pengamanan *file*yang lain seperti Triple Des, RSA, Serpent dan Twofish.
2. Pengujian yang dilakukan pada algoritma Bcrypt masih terbatas menggunakan ronde 10 hingga 20, sebaiknya dicoba menggunakan ronde 21 hingga 31 untuk menguji performa dan kemanaan Bcrypt.
3. Membandingkan dengan algoritma *hashing* lainnya seperti SHA-3, Argon2, SHA2-384 dan SCrypt