BAB V
KESIMPULAN

1.1 Kesimpulan

Kesimpulan dari penelitian Implementasi algoritma *symmetric key* AES menggunakan *hashing* untuk ekspansi kuci dan Blowfish untuk enkripsi dan dekripsi data menggunakan otentikasi OTP pada keamanan data file pada saat akan mengunduh data yang tersimpan adalah sebagai berikut.

1. Enkripsi dan dekripsi terhadap data dengan menggunakan algoritma kriptografi blowfish yang disimpan didalam database dengan ciphertext yang dihasilkan dari enkripsi tersebut sehingga data hanya dapat diunduh apabila user mempunyai akses dengan kode otentikasi yang dikirimkan melalui email yang telah terdaftar.
2. Pada saat user akan mengunduh data yang tersedia maka sistem akan mengirim *One-Time-Password* yang merupakan kombinasi dari *uppercase*, *lowercase*, dan *number* sebanyak 8 digit kemudian *Ciphertext* tersebut dikirimkan melalui email user yang telah terdaftar, setelah user mendapatkan kode otentikasi yang dikirimkan ke email yang telah terdaftar maka user dapat mengunduh file dengan memasukan kode otentikasi pada form yang telah disediakan untuk memasukan kode tersebut ditambah dengan cache sehingga kode otentikasi hanya dapat dipakai satu kali, kode otentikasi yang dimasukan oleh user sistem akan mengecek apakah kode tersebut masih valid atau sudah tidak valid, jika valid *One-Time-Password* tersebut di enkripsi menggunakan algortima AES yang ekspansi kuncinya telah di-*hashing* dengan algoritma SHA-256, dan data file akan di dekripsi menggunakan algoritma blowfish sehingga data file dapat di unduh oleh user.
3. Pengambilan data menggunakan algoritma AES-256 yang dikombinasikan SHA-256 berjalan lancar terbukti dari hasil pengujian black box pada bagian pengujian keseluruhan tidak mengalami error

Yuda Wijaya Prawira, 2018
IMPLEMENTASI ALGORITMA SYMETRIC KEY ADVANCED ENCRYPTION STANDARD (AES) DAN BLOWFISH MENGGUNAKAN OTENTIKASI GENERATE ONE TIME PASSWORD (OTP) PADA KEAMANAN DATA FILE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

4. Kerahasiaan data hasil enkripsi algoritma blowfish terbukti berhasil untuk mengamankan data karena data yang dienkripsi oleh algoritma blowfish tidak

Yuda Wijaya Prawira, 2018
IMPLEMENTASI ALGORITMA SYMETRIC KEY ADVANCED ENCRYPTION STANDARD (AES) DAN BLOWFISH MENGGUNAKAN OTENTIKASI GENERATE ONE TIME PASSWORD (OTP) PADA KEAMANAN DATA FILE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

berhasil di dekripsi oleh pengujian wireshark dalam simulasi serta hasil enkripsi menggunakan algoritma blowfish teracak sangat baik.

1.2 Saran

Berikut merupakan saran pada penelitian ini untuk pengembangan lebih lanjut:

1. Input yang dimasukan tidak hanya berupa data .pdf dan .docx namun juga bisa berupa video dan menyisipkan pesan di dalam berkas tersebut.s
2. Modifikasi untuk algortima *Advanced Encryption Standatd* dapat menggunakan dua prinsip Shannon yaitu *confusion* dan *diffusion* pada bagian *MixXolumn, SubBytes*, atau *AddRoundKey*.