BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian melakukan perancangan, implementasi, pengujian dan analisis penerapan algoritma *Blowfish* dan algoritma *Elgamal* untuk mengamankan data sekunder pada *database* didapatkan kesimpulan sebagai berikut.

1. Penerapan algoritma *Blowfish* dan *Elgamal* pada penelitian ini belum dapat membuktikan tingkat keamanan melalui percobaan. Namun dengan penerapan kombinasi algoritma ini dapat meningkatkan keamanan dengan mempersulit penyerang *database* ketika berusaha memecahkan cipherteks, karena penyerang belum tahu algoritma apa yang digunakan dan dua algoritma tersebut mempersulit *brute force attack* dalam menebak algoritmanya. Kemudian karena kunci yang digunakan ada tiga yaitu kunci *Blowfish*, kunci publik dan kunci privat *Elgamal*. Penggunaan tiga kunci tersebut dapat meningkatkan keamanan dari serangan *exhaustive attack* pada saat mecoba *brute force attack* pada kuncinya karena untuk memecahkan dengan memasukan segala kunci akan memerlukan waktu yang sangat lama dan sulit.
2. Cipherteks dari enkripsi algoritma *Blowfish* dan algoritma *Elgamal* berhasil dekripsi kembali menjadi plainteks data asli yang dapat dilihat dan ditampilkan baik oleh *admin* dan *user*.
3. Penerapan algoritma *Blowfish* dan algoritma *Elgamal* dengan melakukan percobaan enkripsi dan dekripsi menghasilkan peningkatan panjang karakter pada cipherteks dari plainteks sebesar 12 kali lebih panjang pada data nama, sebesar 11 kali lebih panjang pada data alamat, dan sebesar 14 kali lebih panjang pada data nomor telepon. Rata-rata peningkatan panjang dari plainteks dan cipherteks pada penelitian ini yaitu sebesar 12,5 kali peningkatan panjang karakternya.

4. Waktu proses enkripsi dan dekripsi pada penerapan algoritma Blowfish dan algoritma Elgamal penelitian ini memiliki waktu rata-rata yang cukup cepat yaitu 14,86 ms untuk waktu enkripsi dan 12,29 ms waktu dekripsi. Waktu proses dekripsi lebih cepat dibandingkan enkripsi.
5. Penggunaan sumber daya komputer pada penerapan algoritma *Blowfish* dan algoritma *Elgamal* pada penelitian ini memiliki penggunaan pada jarak 3% hingga 9,5 % penggunaan sumber daya CPU .Penggunaan sumber daya komputer RAM sebesar 300 mb hingga 480 mb. Pengujian menggunakan browser Firefox .
6. Berdasarkan *Load testing* yang dilakukan penggunaan optimal dan maksimal pada masukan perangkat lunak pada penelitian ini adalah 32 karakter masukan data sekunder, maksimal 16 karakter kunci *Blowfish* , dan 6 digit angka masukan angka bilangan prima kunci publik. Masukan tersebut menggunakan waktu selama 1,67 detik atau 1674 ms yang masih dapat diterima lama waktunya.
7. Faktor yang mempengaruhi lama waktu proses enkripsi dan dekripsi adalah panjang kunci dimana jika panjang kunci publik memiliki digit yang lebih besar akan meningkatkan waktu proses perhitungan yang lebih besar pada saat proses enkripsi dan dekripsi. Begitu juga dengan kunci *Blowfish* dimana semakin panjang karakternya maka semakin lama waktu yang digunakan pada proses pembangkitan kunci.
8. Faktor perangkat keras CPU dapat mempengaruhi lama waktu penerapan algoritma *Blowfish* dan algoritma *Elgamal* dimana dengan spesifikasi CPU intel i5 lebih lama waktunya dibandingkan dengan CPU intel i7.

5.2 Saran

Adapun saran untuk penelitian selanjutnya yaitu :

1. Penelitian selanjutnya dapat menerapkan kombinasi algoritma kriptografi simetris dan asimetris lainnya agar mendapatkan efisiensi yang lebih baik. Untuk algoritma kriptografi simeteris dapat mengkombinasikan algoritma yang lebih baru setelah algoritma *Blowfish* yaitu Algoritma *Twofish*. Kemudian dapat dikombinasikan dengan algoritma asimetris lainnya seperti RSA.

2. Penerapan untuk kunci publik sebaiknya langsung di konfigurasi oleh *admin* secara langsung sehingga tidak perlu melakukan input kembali oleh *user* karena kunci publik memiliki sifat yang tidak masalah jika diketahui oleh banyak orang.