BAB 6

KESIMPULAN DAN SARAN

Pada bab ini, akan dijelaskan mengenai kesimpulan dari awal hingga akhir penelitian beserta saran untuk penelitian selanjutnya.

6.1 Kesimpulan

Setelah melakukan proses analisis, perancangan, implementasi, dan pengujian pada penelitian ini, maka dapat diambil beberapa kesimpulan, diantaranya:

1. Modifikasi algoritma DES Berbasiskan Graf dilakukan dengan cara menggunakan sirkuit Hamilton sebuah graf sebagai kunci awal dan 16 buah pemetaan graf yang tidak termasuk dalam *graph automorphism* untuk membangun 16 buah kunci ronde.
2. Cara yang digunakan untuk mengimplementasikan algoritma DESBG yaitu membuat sebuah graf pada perangkat lunak, mencari sirkuit Hamilton dari graf tersebut untuk digunakan sebagai kunci awal, dan mencari 16 buah pemetaan untuk digunakan dalam proses pembangunan kunci.
3. Berdasarkan pengujian eksperimental yang telah dilakukan, jumlah maksimal percobaan yang dibutuhkan untuk meretas 16 buah kunci ronde algoritma enkripsi DESBG menggunakan metode *brute force* lebih besar dibandingkan dengan algoritma enkripsi DES. Maka algoritma enkripsi DESBG lebih sulit diretas dibandingkan algoritma DES menggunakan metode *brute force*.

6.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, berikut saran-saran yang dapat diberikan untuk penelitian selanjutnya:

- Perangkat lunak yang dibangun dalam skripsi ini tidak dibuat dalam basis bilangan biner melainkan dalam basis bilangan byte, hal ini disebabkan karena bahasa pemrograman yang digunakan adalah *Java*. Untuk penelitian selanjutnya penulis berharap perangkat lunak dikembangkan untuk dapat melakukan proses enkripsi sesungguhnya dalam basis biner.
- Perangkat lunak yang dibangun pada skripsi ini hanya mampu mengenkripsikan masukan yang ditulis oleh pengguna menggunakan *keyboard*. Untuk penelitian selanjutnya penulis berharap perangkat lunak dikembangkan untuk dapat melakukan proses enkripsi dengan masukan berupa gambar atau file.
- Pengujian yang dilakukan terhadap perangkat lunak yang dibangun pada skripsi ini hanya menggunakan metode *brute force*. Untuk penelitian selanjutnya penulis berharap tipe serangan lain dapat digunakan untuk mengetahui lebih lanjut perbandingan keamanan algoritma DES dan DESBG.

DAFTAR REFERENSI

[1] Munir, R. (2006) *Kriptografi*. Informatika, Bandung.

[2] Rosen, K. H. (2012) *Discrete Mathematics and Its Applications*, 7th edition. McGraw-Hill, New York.

[3] Cameron, P. J. (2005) Automorphisms of graphs. Bagian dari Beineke, L. W. dan Wilson, R. J. (ed.), *Topics in Algebraic Graph Theory*. Cambrige University Press, New York.

[4] Sensarma, D. dan Sarma, S. S. (2014) Gmdes : A graph based modified data encryption standard algoritm with enchanced security. Technical Report eISSN: 2319-1163. University of Calcutta, West Bengal, India.

[5] Stallings, W. (2005) *Cryptography and Network Security*, 4th edition. Prentice Hall, New Jersey.