BAB V
KESIMPULAN DAN SARAN

Pada bab ini akan dipaparkan kesimpulan yang diperoleh dari penelitian yang dilakukan dan saran untuk penelitian mengenai *digital signature* kedepannya.

5.1 Kesimpulan

Berdasarkan hasil penelitian, pengujian, dan analisis terhadap sistem, maka didapatkan kesimpulan sebagai berikut:

1. Implementasi Algoritma ElGamal dalam pembuatan *digitial signature* diterapkan pada proses pembangkitan kunci, proses enkripsi dan proses dekripsi dokumen. Sementara Fungsi SHA-512 *(Secure Hash Algorithm - 512)* diterapkan pada proses perhitungan nilai *hash* dalam pembuatan *digital signature* dan proses verifikasi *digital signature*.

   Analisis terhadap implementasi Algoritma ElGamal dan SHA-512 *(Secure Hash Algorithm - 512)* untuk penanganan *data collision* pada *digital signature* dilakukan melalui empat skenario pengujian dengan *man in the middle attack scenario*, yaitu yang pertama, pembuatan *digital signature* dilakukan dengan menggunakan SHA-512 dan Enkripsi ElGamal. Kedua, pembuatan *digital signature* dilakukan dengan menggunakan SHA-512 dan tanpa Enkripsi ElGamal. Ketiga, pembuatan *digital signature* dilakukan tanpa menggunakan SHA-512 tetapi menggunakan Enkripsi ElGamal. Keempat, pembuatan *digital signature* dilakukan tanpa menggunakan SHA-512 dan Enkripsi ElGamal. Dan hasil analisis dapat terlihat jelas dengan membandingkan hasil pengujian pertama dengan hasil pengujian ketiga, dan membandingkan hasil pengujian kedua dengan hasil pengujian keempat.
2. Fungsi SHA-512 *(Secure Hash Algorithm - 512)* dapat digunakan bersamaan dengan Algoritma ElGamal untuk menangani masalah *data collision* pada *digital signature.*

5.2 Saran

Adapun saran yang ingin penulis sampaikan untuk kepentingan penelitian selanjutnya mengenai *digital signatur* 86 ıh sebagai berikut:

1. Algoritma ElGamal merupakan saıah satu algoritma yang aman digunakan dalam pengamanan pesan atau dokumen. Pada penelitian ini digunakan untuk membangkitkan kunci serta proses enkripsi dan dekripsi dokumen. Meskipun termasuk dalam algoritma yang aman, kunci publik juga harus dijaga keamanannya dengan membuat kunci yang berbeda setiap melakukan pertukaran dokumen atau pesan agar tidak dimanipulasi oleh pihak-pihak yang tidak bertanggungjawab.
2. Untuk kedepannya, pembuatan *digital signature* dengan mengimplementasikan Algoritma ElGamal dan SHA-512 *(Secure Hash Algorithm - 512)* dapat dimanfaatkan untuk semua format *file* dokumen, serta isi dari dokumennya tidak hanya sebatas teks saja, mungkin dokumen bergambar, bahkan yang berisi *audio* atau *video.*
3. Pada penelitian berikutnya diharapkan dapat dilakukan penelitian untuk menganalisis penerapan Algoritma ElGamal pada proses transmisi data, baik data teks, gambar, *audio*, bahkan *video*.
4. Perlu dipelajari berbagai jenis *man in the middle attack* yang mungkin terjadi beserta penanganannya.