BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan data hasil perbandingan algoritma asimetris yang dijelaskan pada BAB IV, dapat disimpulkan bahwa:

1. Pada pengujian waktu enkripsi dan dekripsi dengan panjang kunci 192bit algoritma ElGamal membutuhkan waktu yang paling sedikit, namun ketika dilakukan pengujian dengan panjang kunci 512bit dan 1024bit terjadi kenaikan waktu yang cukup signifikan. Pada proses pembuatan tandatangan digital dengan panjang kunci 192bit, 512bit, dan 1024bit RSA membutuhkan waktu paling sedikit dibandingkan dengan ECC dan ElGamal. Hasil perbandingan waktu menunjukan bahwa algoritma RSA lebih baik dari algoritma ECC dan Elgamal dalam waktu enkripsi, dekripsi, dan tandatangan digital serta memiliki pertumbuhan waktu yang konstan dan tidak mengalami kenaikan yang terlalu besar.

2. Algoritma RSA memiliki nilai kompleksitas tertinggi dengan nilai $O(n^2)$ yang menunjukan bahwa pertumbuhan waktu bernilai kuadratik atau n^2, sehingga untuk setiap pertumbuhan nilai n, akan menghasilkan pertumbuhan waktu senilai n x n. Nilai kompleksitas waktu algoritma ECC dan ElGamal adalah sama dengan nilai O(n log n) yang menunjukan bahwa pertumbuhan waktu bernilai lanjar dikalikan dengan logaritmik, sehingga untuk setiap pertumbuhan nilai n, akan menghasilkan pertumbuhan waktu yang cukup rendah dan memiliki nilai yang mendekati nilai n. Berdasarkan nilai kompleksitas waktu, Algoritma Elgamal dan ECC menjadi algoritma terbaik karena memiliki nilai kompleksitas waktu terendah.

5.2 Saran

Berdasarkan hasil penelitian yang telah dijelaskan, berikut beberapa saran yang selanjutnya dapat digunakan untuk penelitian selanjutnya.

1. Penggunaan kurva pada algoritma ECC yang dapat ditambahkan sehingga dapat dibandingkan dengan algoritma lain dengan panjang kunci yang sama.
2. Pengaruh penggunaan CPU dan memori dalam proses pengujian yang dapat mempengaruhi hasil pengujian, sehingga lebih baik alat pengujian dalam kondisi stabil.
3. Penggunaan variasi masukan dengan berbagai ukuran yang berbeda agar hasil pengujian lebih terlihat perbedaannya.