BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil penelitian yang telah dipaparkan pada Bab IV, dapat ditarik kesimpulan sebagai berikut:

1. Implementasi Algoritma *Elliptic Curve Diffie-Hellman* untuk protokol autentikasi *user* pada *Two Way Challenge Response Protocol* melibatkan lima tahapan utama. Tahapan pertama adalah *user* menentukan kurva eliptik dan titik basis. Tahapan kedua adalah penghitungan P_A oleh *user*. Tahapan ketiga adalah pemberian *challenge* oleh *server* kepada *user*. Tahap keempat yaitu *user* menghitung dan menginput *response* yang diperoleh. Pada tahap kelima, *server* membandingkan *response* yang diinput *user* dengan hasil perhitungannya. Protokol autentikasi selesai jika *response user* benar.
2. Program aplikasi dirancang menggunakan bahasa pemrograman Python versi 3.9. Untuk mengkonstruksi tampilan program digunakan *package tkinter*. *Package openpyxl* digunakan untuk mengakses file database yang telah dibuat. *Package random* digunakan untuk membangkitkan bilangan bulat acak. Modul *Points* digunakan saat inisiasi kurva dan operasi titik, serta modul *Helper* untuk pengecekan syarat kurva eliptik.

5.2 Saran

Adapun saran dari penulis untuk penelitian berikutnya adalah:

1. Mengkaji penggunaan protokol dan skema autentikasi yang telah dikembangkan dalam penelitian ini pada aplikasi lain yang sering dipakai dalam kegiatan sehari-hari, seperti aplikasi perpesanan, sosial media, atau lainnya.

2. Mengembangkan penggunaan Algoritma *Elliptic Curve Diffie-Hellman* untuk protokol autentikasi lainnya seperti *Three Way Challenge-Response Protocol* atau *Trusted Party*.
3. Mengkaji algoritma lainnya yang mungkin diterapkan pada *Two Way Challenge Response Protocol*..