BAB V
SIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Skema pengiriman email menggunakan enkripsi ECDH memilki lima tahapan. Tahap pertama adalah Alice dan Bob (pengirim dan penerima email) menyepakati kurva E serta generator G, tahap kedua adalah Alice dan Bob menetapkan kunci kunci privat masing-masing serta menghitung kunci publik masing-masing, tahap ketiga adalah Alice dan Bob saling menukarkan kunci publik serta menghitung kunci simetri masing-masing, tahap keempat adalah Alice menenkripsi pesan menggunakan kunci simetri serta mengirimkan *ciphertext* ke Bob, tahap kelima adalah Bob memeriksa emailnya lalu mendapatkan *ciphertext* dari Alice dan mendekprisi *chipertext* tersebut.
2. Aplikasi Pengiriman Email Menggunakan Enkripsi ECDH menggunakan bahasa pemograman Python berupa program aplikasi. *Package* yang digunakan dalam pembuatan program di python meliputi *tkinter* untuk tampilan program, *random* untuk pembangkitan kunci, *smtplib* untuk pengiriman email, dan *webbrowser* untuk mempermudah akses izin aplikasi pihak ketiga di gmail. Program komputer tersebut digunakan untuk mempermudah pengguna (pengirim dan penerima pesan email) untuk melakukan pembangkitan kunci, enkripsi, pengiriman email, dan dekripsi. Alur pembuatan program aplikasi secara ringkas yaitu langkah pertama membuat beberapa *function* untuk melakukan kalkulasi perhitungan seperti pada tab pembangkitan kunci, langkah kedua membuat *function* enkripsi dan dekripsi, dan langkah terakhir membuat *function* untuk pengiriman email.

5.2 Saran

Adapun saran dari penulis untuk penelitian ini adalah:

1. Peneliti selanjutnya diharapkan dapat menggunakan pesan selain *text* alfanumerik seperti pesan audio, *file*, dan lain-lain.
2. Penelitian selanjutnya juga diharapkan menggunakan kunci enkripsi selain mengambil absis, dan menggunakan enkripsi selain Cipher Caesar.