BAB V
SIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Kriptosistem gabungan S-ECIES dan RSA merupakan kriptografi kunci publik (kriptografi asimetris) yang memiliki tiga tahapan. Tahap pertama adalah pembangkitan kunci oleh penerima pesan, tahap kedua adalah enkripsi *plaintext* oleh pengirim pesan dan tahap ketiga adalah dekripsi *ciphertext* oleh penerima pesan. Kriptosistem gabungan S-ECIES dan RSA dapat mempersulit kriptanalis dalam melakukan kriptanalisis karena dibutuhkan dua algoritma dengan kompleksitas eksponensial dan sub-eksponensial untuk meretas kriptosistem ini.
2. Implementasi kriptosistem gabungan S-ECIES dan RSA dilakukan menggunakan bahasa pemrograman Python berupa program komputer. Implementasi dilakukan menggunakan kurva P-256 dan RSA dengan modulus 2048-bit. Program komputer tersebut digunakan untuk mempermudah pengguna (baik pengirim maupun penerima pesan) untuk melakukan pembangkitan kunci, enkripsi dan dekripsi.

5.2 Saran

Adapun saran dari penulis untuk penelitian ini adalah:

1. Peneliti selanjutnya diharapkan dapat menganalisa keamanan kriptosistem gabungan S-ECIES dan RSA secara lebih mendalam.
2. Dalam penelitian selanjutnya, dapat dikaji apakah representasi plaintext dapat menggunakan sistem Unicode untuk mendukung huruf-huruf selain huruf Latin dan emoji.
3. Dapat pula dikaji apabila menggunakan kurva eliptik lain yang lebih modern dan lebih cepat seperti Curve25519.