BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan yang telah dipaparkan pada bab-bab sebelumnya, maka diperoleh kesimpulan sebagai berikut:

1) Secara garis besar, terdapat tiga prosedur untuk autentikasi dokumen digital dengan menggunakan *Secure Hash Algorithm*-256 dan ElGamal *Signature Scheme*, yaitu pembangkitan kunci yang di dalamnya terdapat kunci publik dan kunci privat, pembuatan tanda tangan, dan autentikasi dokumen digital. Pembangkitan kunci dilakukan oleh pengirim dokumen untuk membuat tanda tangan digital yang kemudian dikirimkan ke penerima dokumen, sedangkan pengirim dapat melakukan autentikasi dokumen hanya dengan kunci publik pengirim dan tanda tangan pengirim.
2) Program aplikasi dirancang dengan dua menu utama, yaitu menu "SIGNING" dan "VERIFYING". Menu *signing* digunakan untuk membuat tanda tangan digital, sedangkan menu *verifying* digunakan untuk autentikasi dokumen digital. Pada menu *signing* dibuat label pembangkitan kunci yang bertujuan memudahkan pengguna dalam memilih bilangan-bilangan acak untuk kebutuhan pembuatan tanda tangan digital.

5.2 Saran

Adapun saran dari penulis untuk penelitian ini adalah:

1) Penulis menyarankan dalam prosedur pembangkitan kunci, kunci publik dibuat berbeda-beda untuk setiap pengiriman dokumen agar dokumen tidak mudah dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab.
2) Dalam merancang program aplikasi autentikasi dokumen digital dengan menggunakan SHA-256 dan ElGamal *Signature Scheme* berbantuan Python, penulis menyarankan untuk menggunakan modul fungsi *hash*

untuk SHA-256 yang telah tersedia di Python untuk memudahkan proses pengkodingan.