BAB V
KESIMPULAN DAN SARAN

Bagian ini membahas terkait kesimpulan dari penelitian yang telah dilakukan dan saran yang dapat digunakan untuk penelitian selanjutnya.

5.1 Kesimpulan

Berdasarkan rumusan masalah dan pembahasan hasil penelitian yang telah diuraikan pada bab sebelumnya, diperoleh kesimpulan sebagai berikut.

1. Skema penggabungan fungsi hash jenis SHA-256 (*Secure Hash Algorithm*-256) dan algoritma kriptografi kunci asimetri RSA (*Rivest-Shamir-Adleman*) yang ditingkatkan dimulai dengan menambahkan satu bilangan prima pada proses pembangkitan kunci. Di samping mempercepat proses enkripsi dan dekripsi *message digest*, adanya peningkatan algoritma RSA dalam proses pembuatan program aplikasi dapat lebih menjaga keamanan dan keaslian sebuah tanda tangan pada dokumen digital dari oknum yang tidak berkepentingan. Selain itu, penggunaan QR Code menjadi salah satu cara agar proses akses tanda tangan digital dan autentikasinya lebih mudah.
2. Program aplikasi autentikasi tanda tangan pada dokumen digital dapat dibuat dengan *Graphical User Interface* (GUI) Python untuk menghasilkan program aplikasi yang *user-friendly*. Terdapat tiga menu utama, yaitu menu *key generator*, *signing*, dan *verifying*. Menu *key generator* dan *signing* dapat digunakan oleh pengirim dokumen untuk membuat tanda tangan digital. Sementara itu, menu *verifying* dapat digunakan oleh penerima dokumen untuk melakukan autentikasi keaslian tanda tangan pada dokumen digital. Keluaran utama dari program aplikasi ini adalah sebuah penjelasan terkait keaslian dan kecocokan tanda tangan pada dokumen digital. Jika keduanya autentik, program aplikasi akan memunculkan beberapa informasi terkait tanda tangan digital, seperti waktu penandatanganan, nama pemberi tanda tangan, dan tempat dokumen ditandatangani. Jika keduanya tidak autentik, program aplikasi akan memunculkan beberapa kemungkinan alasan, seperti tanda tangan tidak valid, terjadi perubahan isi dokumen, serta dokumen dan tanda tangan tidak cocok.

5.2 Saran

Adapun saran yang dapat diterapkan untuk penelitian selanjutnya, yaitu:

1. Pada penelitian ini, digunakan penggabungan algoritma RSA yang ditingkatkan dan SHA-256. Untuk penelitian selanjutnya, disarankan penggunaan gabungan algoritma dan fungsi hash lainnya, seperti *Elliptic Curve Digital Signature Algorithm* (ECDSA) dan SHA-512. Selain itu, disarankan adanya pengkajian terkait kelebihan dan kekurangan dari setiap algoritma sehingga mendapatkan algoritma terbaik untuk autentikasi dokumen digital menggunakan QR Code.
2. Pada penelitian ini, *input* dalam proses autentikasi dokumen digital pada program aplikasi berupa dokumen dan tanda tangan yang terpisah, serta *output* berupa beberapa kemungkinan alasan ketika dokumen dan tanda tangan tidak autentik. Untuk penelitian selanjutnya, disarankan adanya pengembangan kode pada program aplikasi sehingga *input* dalam proses autentikasi dokumen digital pada program aplikasi hanya berupa dokumen digital dengan tanda tangan yang sudah disisipkan, serta *output* berupa penjelasan khusus berdasarkan kesalahan *input* sehingga penjelasan tidak terlalu umum ketika dokumen digital dan tanda tangan tidak autentik.