BAB V
KESIMPULAN

Berdasarkan rumusan masalah dan pembahasan hasil penelitian sebagaimana yang telah dipaparkan pada bab sebelumnya maka diperoleh kesimpulan dan saran dari hasil penelitian tersebut.

5.1 Kesimpulan

Kesimpulan yang diperoleh dari hasil penelitian yang telah diuraikan sebelumnya antara lain sebagai berikut.

1. Perancangan skema autentikasi tanda tangan digital menggunakan kriptografi RSA dan fungsi *hash* BLAKE2 memiliki tiga proses utama, yaitu pembangkitan kunci, *signing* atau penandatangan dokumen digital, dan *verifying* atau proses autentikasi dokumen digital. Dari proses pembangkitan kunci akan dihasilkan sepasang kunci publik yang akan digunakan dalam proses tanda tangan dan kunci privat yang akan digunakan dalam proses autentikasi tanda tangan. Selain itu, tanda tangan digital menggunakan fungsi *hash* BLAKE2 dengan skema penandatanganan RSA yang diterapkan pada dokumen digital berformat .pdf.
2. Program aplikasi *digital signature* kriptografi RSA dan fungsi *hash* BLAKE2 dikonstruksi dalam bentuk *webpage* yang dapat diakses pada url http://54.88.151.217/ yang dibuat menggunakan bahasa pemrograman Python serta HTML. Dalam *webpage* tersebut pengguna dapat melakukan pembangkitan kunci, tanda tangan digital dokumen digital, serta verifikasi tanda tangan digital dari dokumen digital yang diunggah.

5.2 Saran

Adapun saran penulis untuk penelitian ini adalah:

1. Dapat dilakukan penelitian lebih lanjut mengenai bentuk implementasi lain dari aplikasi tanda tangan digital menggunakan fungsi *hash* BLAKE2 dan kriptografi RSA, seperti implementasi dalam bentuk *software* aplikasi atau aplikasi *mobile.*
2. Penelitian lebih lanjut di mana penggunaan fungsi *hash* BLAKE2 bisa dikombinasikan dengan skema penandatanganan lainnya.

3. Hasil penelitian dapat diimplementasikan pada suatu instansi atau perusahaan yang membutuhkan verikasi keaslian suatu dokumen digital.