BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

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

1. Penggunaan fungsi *hash* SHA-256 dan algoritma kriptografi RSA pada aplikasi *E-Voting* berbasis web ini merupakan penggabungan antara skema protokol kriptografi dengan tanda tangan digital. Skema dari protokol kriptografi berfungsi untuk menjaga kerahasiaan dari pilihan yang masuk, sedangkan protokol tanda tangan digital berfungsi untuk menjaga integritas dan nirpenyangkalan.
2. Program aplikasi *E-Voting* berbasis web ini dibuat dengan bahasa pemrograman javascript untuk menghasilkan program aplikasi yang *user-friendly*. Terdapat empat halaman utama, yaitu halaman admin, registrasi pemilih, *voting* serta registrasi panitia. Halaman admin digunakan untuk mengunggah data pemilih serta data panitia.
3. Pada tahapan validasi ada beberapa validasi yang dilakukan pada setiap halaman. Halaman registrasi pemilih jika pemilih sudah terdaftar maka akan bisa melakukan pemilihan, sesudah melakukan registrasi maka data pemilih akan diunggah secara otomatis ke dalam *database* yang sudah berbentuk token, lalu pemilih akan memasuki halaman *voting* untuk menentukan pilihannya, hasil pemilihan tersebut akan diunggah ke *database* yang sudah terenkripsi bersama token yang sudah ada. Token dan hasil dekripsi dari hasil pemilihan dicocokan pada halaman validasi, jika token serta hasil dekripsi cocok maka suara tersebut sah. Aplikasi berjalan dengan baik karena pada penyamaan token dengan hasil dekripsi dari hasil pemilihan tidak terjadi perubahan pada tanda tangan digital nya.

5.2 Saran

Adapun saran yang dapat diterapkan untuk penelitian selanjutnya, yaitu:

Pada penelitian ini, digunakan penggabungan RSA dan SHA-256. Untuk penelitian selanjutnya, disarankan penggunaan gabungan algoritma dan fungsi hash lainnya, seperti RSA yang ditingkatkan atau *Elliptic Curve Cryptography* dan SHA-512. Selain itu, disarankan adanya pengkajian terkait kelebihan dan kekurangan dari setiap algoritma yang dipakai pada penilitian ini sehingga mendapatkan algoritma terbaik untuk *E-Voting* berbasis web. Penelitian selanjutnya diharapkan dapat mengembangkan protokol *e-voting* dengan menggunakan metode lain seperti pertukaran kunci.