BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Adapun kesimpulan akhir dari penelitian Sistem E-voting menggunakan protokol *Two Central Facilities* dengan menggabungkan algoritma AES dan RSA sebagai kombinasi keamanan

1. Protokol *Two Central Facilities* dalam sistem *e-voting* yang dibangun memenuhi kriteria yang ditetapkan oleh Scheiner. Protokol *Two Central Facilities* dapat meminimalisir kecurangan, bahkan oleh pihak-pihak penyelenggara, yaitu CLA dan CTF. Dengan dipisahkannya database untuk menyimpan data pemilih dan data hasil pemilihan, maka pihak CLA tidak mengetahui kandidat mana yang dipilih oleh pemilih, dan pihak CTF tidak mengetahui siapa yang memilih kandidat yang mana. Jika kedua data diaudit, maka akan ketahuan apabila ada pihak penyelenggara melakukan kecurangan. Kecuali kedua pihak penyelengara melakukan kerjasama. Namun pada penelitian kali ini, proses komunikasi data belum manggunakan jalur komunikasi yang aman.
2. Dengan digunakannya algoritma AES dan RSA, maka proses pengiriman data menjadi lebih terjaga karena data yang dikirimkan adalah data yang telah dienkripsi sebelumnya, bukan data yang sebenarnya. Sehingga jika terjadi pencurian data, pencuri data tersebut masih harus melakukan proses dekripsi menggunakan kunci yang digunakan untuk proses dekripsi. Penggunaan algoritma AES dan RSA berpengaruh terhadap waktu eksekusi yang diperlukan oleh sistem. Waktu yang diperlukan untuk melakukan pengaksesan terhadap sistem yang menggunakan proses

enkripsi dan dekripsi adalah 39 menit 49 detik, sedangkan untuk pengaksesan sistem yang tidak menggunakan enkripsi hanya 17 menit 11 detik. Terlebih pada saat proses penghitungan suara, karena semua data pilihan yang disimpan di dalam database telah dienkripsi sehingga untuk melakukan proses penghitungan suara, setiap *record* pilihan harus didekripsi terlebih dahulu. Namun, tidak semua tujuan kriptografi terpenuhi oleh implementasi algoritma AES dan RSA, hanya poin kerahasiaan yang tercapai sepenuhnya.

5.2. Saran

Untuk pengembangan lebih lanjut, saran-saran yang diberikan pada penelitian ini:

1. Proses autentikasi lebih aman jika tidak menggunakan username dan password, melainkan menggunakan *smart card* atau sidik jari.
2. Melakukan perubahan bahasa pemrograman dari PHP ke bahasa lainnya, seperti java atau python yang lebih cepat dalam hal eksekusinya, karena algoritma RSA yang digunakan dalam penelitian ini masih menggunakan kunci yang relative kecil ukurannya. Sedangkan menurut beberapa penelitian sebelumnya, panjang kunci RSA yang diperkirakan aman adalah lebih dari 1024-bit.
3. Perlu dilakukan penelitian dan pemodifikasian lebih lanjut terhadap protokol *Two Central Facilities* agar dapat digunakan di Indonesia sesuai dengan peraturan-peraturan tentang pemilihan umum yang berlaku di Indonesia.
4. Jalur komunikasi data menggunakan *secure chanel* sehingga lalu lintas data menjadi lebih aman.