BAB V

PENUTUP

5.1 Kesimpulan

Algoritma RC4 merupakan salah satu algoritma Kode Rivest yang dapat digunakan untuk mengamankan data-data sensitif dalam sebuah sistem informasi, karena algoritma kriptografi ini mampu memberikan solusi agar data yang ada dalam sistem informasi terjaga selama proses pengiriman dan penerimaan data antara client-web server. RC4 dipilih karena keamanan, kecepatan dan prinsip kerjanya dengan algoritma Kode Rivest yang lain. RC4 mentransformasikan inputan data dalam bentuk *byte* seketika pada suatu saat sehingga proses kerja yang dilakukan lebih cepat, dan tidak membutuhkan spesifikasi *hardware* yang tinggi. Hal ini telah dibuktikan pada pengujian yang sudah dilakukan pada penelitian-penelitian sebelumnya.

Adapun modifikasi yang dilakukan adalah mengganti *initialization vector* dengan nilai random yang dihasilkan dari proses *seed random* dengan menggunakan alfanumerik sebagai variabelnya. Hal ini dilakukan untuk mengantisipasi serangan yang dilakukan yaitu *bit flipping attack* dan serangan dengan meng-XOR-kan kedua *cipher* yang memiliki *initialization vector* yang sama untuk mendapatkan XOR dari dua buah plainteks.

Pembuatan sistem pemilihan Ketua BEM yang berbasis komputer dengan implementasi algoritma RC4 ini terdiri dari 2 modul, yakni modul pemilih dan

modul admin. Kedua modul ini memiliki keterhubungan dalam proses pemilihan Ketua BEM. Modul pemilih merupakan modul utama yang digunakan pemilih untuk melakukan pemilihan kandidat calon, modul ini terdiri dari detail kandidat dan pilih kandidat, sedangkan modul admin digunakan untuk manajemen data pemilu, modul ini terdiri dari manajemen data pemilih, manajemen data kandidat calon, data pilihan pemilih (dalam bentuk *cipher*), tabel dan grafik perolehan, dan manajemen kunci/*key* RC4.

Hasil akhir dari proses pemilihan berupa laporan jumlah perolehan suara yang direpresentasikan dalam bentuk tabel dan grafik.

5.2 Saran

Untuk membangun suatu sistem pemilu yang ideal dibutuhkan banyak hal, mulai dari batasan-batasan yang bersifat fleksibel yang diberikan terhadap sistem, keamanan dari sistem itu sendiri dan hal-hal lain yang dianggap penting untuk mendukung kinerja sistem itu sendiri. Hal ini dimaksudkan agar sistem benar-benar dapat dimanfaatkan, baik dari segi konten maupun fitur yang ditawarkan oleh sistem.

Adapun algoritma RC4 yang telah dipaparkan oleh penulis merupakan salah satu metode yang dianggap cocok untuk melindungi data sensitif seperti data pilihan pemilih dalam sebuah sistem pemilihan.