

ABSTRAK

Dewasa ini penggunaan *electronic voting* dalam suatu pemilihan sudah banyak diterapkan sebagai pengganti sistem voting konvensional. Terlepas dari manfaat penggunaan sistem tersebut, pada kenyataannya masih banyak permasalahan yang dapat terjadi, baik dari sisi kesalahan sistem, keamanan jaringan, kerahasiaan data, dan sebagainya. Salah satu masalah utamanya adalah tidak terjaminnya kerahasiaan dan keakuratan data yang tersimpan dan yang akan diproses. Kriptografi sebagai ilmu tentang teknis matematis untuk mengamankan pesan menawarkan solusi atas permasalahan terkait.

Dalam tugas akhir ini dibahas penawaran solusi berupa penggunaan kriptografi atas permasalahan pada sistem keamanan *e-voting*. Pada penelitian ini akan digunakan algoritma kriptografi *Okamoto-Uchiyama* untuk menjamin keamanan dan kerahasiaan data suara, serta memanfaatkan sifat *homomorphic* dari algoritma ini untuk melakukan penghitungan suara. Algoritma ini akan menyembunyikan data dengan mengenkripsi suara yang dipilih oleh pemilih dan sistem dapat melakukan penghitungan menggunakan data yang masih terenkripsi tanpa harus didekripsi terlebih dahulu.

Berdasarkan pengujian pada tugas akhir ini, sistem dapat melakukan enkripsi terhadap data pilihan, menghasilkan *ciphertext* dengan ukuran 3 kali lebih besar dari *plaintext*, dengan lama waktu pemrosesan enkripsi rata-rata 387799,2 *nanoseconds*, dan menghasilkan masing-masing nilai *ciphertext* yang berbeda. Dapat melakukan penghitungan secara *homomorphic* dan menghasilkan keluaran sesuai dengan data yang diinginkan setelah didekripsi.

Kata Kunci : *E-voting*, Kriptografi, Okamoto-Uchiyama, *Homomorphic*.