ABSTRAK

Teknologi telah dimanfaatkan dalam berbagai aspek, baik secara *online* maupun *offline*. Perkembangan pesat teknologi khususnya dalam bidang penyimpanan data secara online dengan sistem awan *(cloud system),* menjadikan jaminan keamanan data sebagai salah satu kebutuhan pokok bagi pemakainya. Terdapat berbagai cara untuk melindungi data yang tersebar secara bebas, salah satunya dengan melakukan enkripi data. Enkripsi adalah proses merubah bentuk data atau informasi ke dalam bentuk lain, yang hanya dapat dibaca oleh penerima yang telah ditentukan oleh sang pengirim. Sang penerima harus memiliki kunci untuk membukanya, disebut sebagai proses dekripsi. Pemanfaatan teknologi tersebut dalam proses pemilihan umum telah dilakukan dengan adanya sistem pemilihan elektronik (*e-voting* system). Namun masalah keamanan adalah sesuatu yang cukup berisiko, sehingga *e-voting* menerapkan sistem keamanan enkripsi data. Hal ini bertujuan untuk menjaga suara pemilih agar tidak diinterupsi oleh baik pihak luar maupun pihak dalam.

Pada tugas akhir ini dirancang sistem keamanan *e-voting* dengan memanfaatkan algoritma enkripsi Paillier yang memiliki sifat *additive homomorphic*. Sifat *homomorphic* membuat sistem dapat melakukan perhitungan suara dalam keadaan terenkripsi tanpa harus mendekripsinya terlebih dahulu, sehingga sistem tidak mengetahui pilihan kandidat tiap pemilihnya. Hal ini dapat menghindari tindakan oknum yang berniat mencurangi proses pemilihan.

Hasil pengujian pada sistem yang telah dibangun menunjukkan sistem dapat melakukan proses enkripsi dan dekripsi secara *homomorphic* terhadap data pilihan dengan waktu pemrosesan enkripsi 3652319 *nanosecond* atau 0.003651 detik dan waktu dekripsi 1499519 *nanosecond* atau 0.001499 detik. Nilai *ciphertext* yang dihasilkan berbeda walaupun *plaintext* yang dienkripsi bernilai sama, dengan ukuran 4 kali lebih besar dari ukuran *plaintext*. Rasio keberhasilan sistem dapat melakukan perhitungan dengan baik yaitu 100%, dengan jumlah maksimal pesan yang dapat dihitung yaitu 3.287.973.778 pesan.

Kata Kunci: Enkripsi, Paillier, *Homomorphic, E-voting,* Keamanan