

ABSTRAK

Dengan berkembangnya teknologi setiap orang dituntut harus dapat menggunakan internet. Salah satu dampak baik dari berkembangnya internet adalah memudahkan seseorang bertukar informasi dan berkomunikasi melalui internet, perkembangan internet juga memberikan dampak negatif yaitu adanya kejahatan dunia maya yang membahayakan informasi pribadi kita. Setiap data yang sifatnya privasi dapat dilihat oleh orang yang tidak berkepentingan. Salah satu cara mencegahnya, dengan membuat informasi yang sifatnya privasi tidak dapat dibaca oleh orang yang tidak berkepentingan dengan kriptografi, kriptografi digunakan untuk mengamankan informasi, termasuk menjaga kerahasiaan, integritas, dan keabsahan data. Kriptografi menggunakan berbagai algoritma seperti enkripsi, hash, dan tanda tangan untuk mencapai tujuan keamanan informasi. Dengan enkripsi informasi yang tadinya mudah dibaca diubah menjadi kumpulan tulisan yang tidak bisa dipahami atau disebut *ciphertext*. Untuk itu diperlukan algoritma untuk melakukan enkripsi dan meningkatkan keamanan suatu data, algoritma *ElGamal* merupakan salah satu algoritma kriptografi yang dapat digunakan untuk melakukan enkripsi. Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskrit pada grup pergandaan bilangan bulat, modulo, dan bilangan prima. Penelitian ini bertujuan mengimplementasikan algoritma *ElGamal* dan meningkatkan keamanan. Hasil akhir dari implementasi algoritma *ElGamal* pada penelitian ini yaitu algoritma *ElGamal* dapat mengenkripsi pesan dengan baik dan berdasarkan pengujian algoritma *ElGamal computational cost* dari segi *memory cost* dapat disimpulkan bahwa penggunaan memori pada aplikasi pengiriman pesan ini tidak memerlukan banyak memori dan berdasarkan hasil dari *time cost* disimpulkan bahwa waktu yang dibutuhkan untuk melakukan enkripsi kecil dan linear. Hasil pengujian MITM untuk meningkatkan keamanan pesan yang dikirim tidak dapat dibaca oleh penyerang.

Kata Kunci: *El-Gamal, Ciphertext, computational cost, memory cost, time cost, MITM* .