ABSTRAK

Bahary, **Barra Rizki**. 2010. *Pengamanan Pesan Teks Menggunakan Algoritma ElGamal*. Skripsi Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Semarang.
Dosen Pembimbing I : Dra. Kristina Wijayanti, M.S.; Dosen Pembimbing II: Isnarto, S.Pd, M.Si.

Kata Kunci: Kriptografi, ElGamal, algoritma asimetris, masalah logaritma diskret, *cipher block*, enkripsi, dekripsi.

Algoritma ElGamal merupakan algoritma kriptografi asimetris yang menggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Kunci publik berfungsi untuk mengenkripsi pesan sedangkan kunci rahasia berfungsi untuk mendekripsi pesan. Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskret pada grup pergandaan bilangan bulat modulo prima, $\mathbb{Z}_p^*=\{\mathbf{1,2,...,}\boldsymbol{p}\mathbf{-1}\}$, dengan p bilangan prima yang dapat dibentuk kedalam $p=2.q+1$ dimana q juga merupakan bilangan prima. Bilangan p seperti itu disebut dengan bilangan prima aman. Apabila digunakan bilangan prima aman dan logaritma diskret yang besar, maka upaya untuk membongkar kunci rahasia akan menjadi lebih sulit.

Algoritma ElGamal mempunyai kunci publik berupa urutan tiga bilangan dan sebuah bilangan sebagai kunci rahasia. Algoritma ElGamal merupakan *cipher block*, yaitu melakukan proses enkripsi pada blok-blok *plaintext* dan menghasilkan blok-blok *ciphertext* yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi.

Kelebihan algoritma ElGamal adalah suatu *plaintext* yang sama akan dienkripsi menjadi *ciphertext* yang berbeda-beda, tetapi pada proses dekripsi akan diperoleh *plaintext* yang sama.

Pada skripsi ini pembahasan difokuskan pada pengaplikasian algoritma ElGamal dalam pengamanan pesan teks dan pengimplementasian algoritma ElGamal kedalam program sederhana menggunakan bahasa pemprograman pascal.

Kajian tentang algoritma ElGamal masih dapat diperluas menjadi tanda tangan digital algoritma ElGamal. Fungsi dari tanda tangan digital ElGamal agar pesan yang sudah dikodekan dengan algoritma ElGamal tetap terjaga dari upaya manipulasi oleh pihak-pihak yang tidak bertanggung jawab.