ABSTRAK

Kriptografi merupakan ilmu yang mempelajari kerahasiaan pesan. Berdasarkan jenis kuncinya, kriptografi dibedakan menjadi dua yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Salah satu algoritma kriptografi kunci asimetris adalah algoritma kriptografi Elgamal. Tujuan dari penelitian ini adalah menyelidiki kriteria pemilihan bilangan prima pada pembentukan kunci algoritma kriptografi Elgamal dan *ciphertext* yang dihasilkan dari sepasang kunci publik algoritma kriptografi Elgamal dengan menggunakan data teks. Berdasarkan hasil penelitian diperoleh kriteria pemilihan bilangan prima pada pembentukan kunci algoritma kriptografi Elgamal yaitu bilangan prima $p > m_i$, dengan m_i adalah blok *plainteks* ke-i. *Ciphertext* yang dihasilkan pada proses enkripsi algoritma kriptografi Elgamal tidak tunggal.

Kata kunci: Kriptografi, Kriptografi Kunci Asimetris, Algoritma Kriptografi Elgamal.

ABSTRACT

Cryptography is the study of the confidentiality of messages. Based on the type of key, cryptography is divided into two, namely symmetric key cryptography and asymmetric key cryptography. One of the asymmetric key cryptographic algorithms is the Elgamal cryptographic algorithm. The purpose of this study was to investigate the selection criteria for prime numbers in the formation of the Elgamal cryptographic algorithm key and the ciphertext generated from a pair of Elgamal cryptographic algorithm public keys by using text data. Based on the results of the research, the criteria for selecting prime numbers in the formation of the Elgamal cryptographic algorithm key are prime numbers $p > m_i$*, where* m_i *is the* i^{th} *plaintext block. The ciphertext generated in the Elgamal cryptographic algorithm encryption process is not single.*

Keywords*: Cryptography, Asymmetric Key Cryptography, Elgamal Cryptographic Algorithm.*