

ABSTRAK

Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan dan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Dengan kata lain kriptografi melakukan penyandian terhadap teks asli menjadi teks sandi. Untuk melakukan penyandian terhadap teks asli menjadi teks sandi (enkripsi) atau mengubah kembali teks sandi menjadi teks asli (dekripsi) diperlukan kunci publik dan kunci rahasia. Salah satu sistem kriptografi adalah sistem kriptografi Elgamal. Sistem kriptografi Elgamal merupakan sistem kriptografi dengan kunci asimetri, dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk dekripsi. Untuk menerapkan sistem kriptografi Elgamal, akan dibuat sebuah aplikasi enkripsi file teks. Aplikasi ini dilengkapi dengan proses enkripsi dan dekripsi dengan sistem kriptografi Elgamal terhadap isi file tersebut untuk mengetahui bagaimana pembangkitan kunci publik, kunci rahasia serta untuk mengetahui besarnya perubahan isi data begitu juga dengan waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

Kata Kunci : Kriptografi Elgamal, Enkripsi, Dekripsi, Kunci Publik, Kunci Rahasia.

ABSTRAK

Cryptography is the science that is based on mathematical techniques for dealing with security and information such as confidentiality, integrity and authentication of data entities. In other words, perform cryptographic encryption of the original text into ciphertext. To perform the encryption of the original text into cipher text (encryption) or change the cipher text back into the original text (decrypted) required public key and private key. One cryptosystem is the ElGamal cryptographic systems. ElGamal cryptographic system is a key cryptosystems with asymmetry, where different keys for encryption with a key for decryption. To implement the ElGamal cryptosystem, will be created a text file encryption applications. The application comes with encryption and decryption with ElGamal cryptosystems to the contents of the file to determine how the public key generation, as well as the secret key to determine the contents of the data changes as well as the time required to perform the encryption and decryption process.

Key Words : ElGamal Cryptographic, Encryption, Decryption, Public Key, Private Key.