

ABSTRAK

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: “*cryptos*” artinya “secret” (rahasia), sedangkan “*graphein*” artinya “writing” (tulisan). kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Menjaga kerahasiaan data dengan kriptografi, data sederhana yang dikirim (*plaintext*) diubah ke dalam bentuk data sandi (*ciphertext*), kemudian data sandi tersebut hanya dapat dikembalikan ke bentuk data sebenarnya hanya dengan menggunakan kunci (*key*) tertentu yang dimiliki oleh pihak yang sah saja. Tujuan kriptografi adalah kerahasiaan, integritas, autentikasi dan nirpenyangkalan. Proses menyandikan plaintext menjadi ciphertext disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan ciphertext menjadi plaintext semula dinamakan dekripsi (*decryption*) atau *deciphering*. Enkripsi dan dekripsi dapat diterapkan baik pada pesan yang dikirim maupun pada pesan tersimpan. Citra digital adalah representasi dari citra dua dimensi menggunakan ‘0’ dan ‘1’ (biner). Citra digital dapat dibedakan menjadi dua, yaitu raster dan vektor. Umumnya yang disebut dengan citra digital adalah citra digital dalam bentuk raster atau yang biasa disebut dengan citra bitmap. File citra digital merupakan suatu file yang bisa saja bersifat pribadi dan rahasia, maka perlu adanya suatu aplikasi sebagai alat bantu yang dapat mengamankan file bersifat pribadi tersebut. Aplikasi enkripsi dan dekripsi diharapkan dapat membantu dalam menjaga kerahasiaan file berbentuk citra digital. Pembuatan sistem menggunakan metode *Extreme Programming* menggunakan bahasa pemrograman yang digunakan adalah PHP.

Kata Kunci: Citra, Digital, Dekripsi, Enkripsi, Kriptografi.