INTISARI

ENKRIPSI DAN DEKRIPSI CITRA DIGITAL *GRAYSCALE* MENGGUNAKAN KRIPTROGRAFI KURVA ELIPTIK DIFFIE-HELLMAN

Oleh

RESTI ANISA LESTARI

14/366128/PA/16214

Dalam skripsi ini dibahas suatu metode untuk menyelesaikan masalah enkripsi dan dekripsi citra digital *greyscale*, yaitu menggunakan kriptografi kurva eliptik Diffie-Hellman. Matriks piksel dari citra yang akan dikirim direpresentasikan pada titik kurva eliptik. Titik-titik tersebut diubah menjadi titik cipher dengan menggunakan proses penjumlahan dan perkalian skalar di dalam kurva eliptik. Hasil dari penjumlahan tersebut direpresentasikan kembali menjadi matriks piksel cipher citra tersebut. Proses berlaku sebaliknya, dengan titik cipher dijumlahkan dengan invers dari kunci rahasia yang dimiliki kedua pihak. Lebih lanjut, untuk mengilustrasikan metode ini, akan diselesaikan suatu contoh enkripsi citra digital *grayscale*.

ABSTRACT

DIGITAL IMAGE GRAYSCALE ENCRIYPTION AND DECRYPTION USING ELLIPTIC CURVE DIFFIE-HELLMAN CRYPTOGRAPHY

By

RESTI ANISA LESTARI

14/366128/PA/16214

This undergraduate thesis discusses a method for solving encryption and decryption of grey scale image, using elliptic curve Diffie-Hellman cryptography. The pixel matrix of the image to be sent is represented at the point of the elliptic curve. These points are converted into cipher points by using the process of addition and scalar multiplication in the elliptic curve. The result of the calculation is represented again into a pixel matrix of the image cipher. The process works the other way around, with the cipher points added up by the inverse of the secret key that both parties have. Furthermore, to illustrate this method, we will complete an example of encryption of a digital image gray scale.