Implementasi Kriptografi Gambar Menggunakan Kombinasi Algoritma Elgamal dan Mode Operasi ECB (Electronic Code Book)

DELVA RIZAL
(Pembimbing : T. Sutojo, S.Si, M.Kom)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201207108@mhs.dinus.ac.id

ABSTRAK

Studio foto Aura photography merupakan suatu usaha yang bergerak di berbagai bidang seperti studio foto, fotocopy dan warnet. Studio ini memiliki satu komputer server dan delapan komputer client (warnet), dimana komputer server digunakan untuk menyimpan berbagai file penting, khususnya file gambar berekstensi .jpg dan .jpeg. Namun penggunaan komputer server tidak hanya karyawan saja, sehingga dalam pengaksesan data penting yang disimpan mudah diakses oleh orang lain yang tidak memiliki hak atas data tersebut. Oleh karena itu, untuk mengamankan file tersebut dibutuhkan pemanfaatan kriptografi dengan mengkombinasikan algoritma Elgamal dan mode operasi ECB dalam melakukan enkripsi dan dekripsi. Penelitian ini memilih kedua algoritma tersebut karena Elgamal merupakan algoritma asimetris serta menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit sedangkan ECB adalah mode operasi yang digunakan dengan kemampuan dekripsi dan enkripsi yang tepat. Sehingga dalam menggunakan kedua algoritma ini dapat memperkuat pengamanan file gambar dan menyulitkan kriptanalis dalam memecahkan file yang terenkripsi. Namun untuk file gambar yang sudah diserang seperti penambahan Brightness atau contrass, noise, blurring dan cropping tidak dapat di dekripsi karena intesitas nilai piksel pada chipertext berubah. Hasil pengujian dari gambar sebelum enkripsi dan sesudah enkripsi dekripsi yaitu MSE 0 dan PSNR inf.

Kata Kunci : Kriptografi, Elgamal, ECB dan File Gambar.

IMPLEMENTATION OF IMAGES CRYPTOGRAPHY USING ELGAMAL ALGORITHM AND ECB MODE OF OPERATION

DELVA RIZAL
(Lecturer : T. Sutojo, S.Si, M.Kom)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201207108@mhs.dinus.ac.id

ABSTRACT

Aura photo studio photography is a business engaged in various fields such as photo studio, photocopy and Internet cafe. The studio has a computer server and client computer eight (cafe), wherein the computer server used to store various important files, particularly image file extension .jpg and .jpeg. However, the use of a computer server not only employees only, so in accessing critical data stored easily accessed by others who do not have rights to the data. Therefore, to secure the files necessary to combine the use of cryptographic algorithms and modes of operation ECB ElGamal in encryption and decryption. This study chose the latter because ElGamal algorithm is asymmetric algorithms and key strength focuses on solving the discrete logarithm problem while the ECB is a mode of operation that is used by the decryption and encryption capability right. So that in using two algorithms can strengthen the security of image files and complicate cryptanalyst in solving the encrypted files. But for the images file that has been attacked like Brightness or contrass addition, noise, blurring and cropping can not be decrypted because the intensity of the pixel values of the ciphertext changed. The results from the image before encryption and after decryption encryption that MSE PSNR 0 and inf.

Keyword : Cryptography, ElGamal, ECB and Images file