KRIPTOGRAFI VISUAL PADA GAMBAR BERWARNA (RGB) MENGGUNAKAN ALGORITMA *ELLIPTIC CURVE CRYPTOGRAPHY*

Skripsi

diajukan untuk memenuhi sebagian syarat untuk memperoleh
gelar Sarjana Matematika

Della Annisa Zahra
NIM 1603362

PROGRAM STUDI MATEMATIKA
DEPARTEMEN PENDIDIKAN MATEMATIKA
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA
BANDUNG
2020

==========

KRIPTOGRAFI VISUAL PADA GAMBAR BERWARNA (RGB) MENGGUNAKAN ALGORITMA ELLIPTIC CURVE CRYPTOGRAPHY

Oleh
Della Annisa Zahra

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Matematika pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

Universitas Pendidikan Indonesia
Agustus 2020

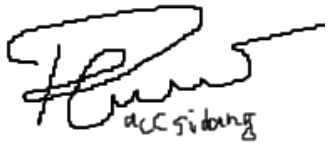
LEMBAR PENGESAHAN

DELLA ANNISA ZAHRA

KRIPTOGRAFI VISUAL PADA GAMBAR BERWARNA (RGB) MENGGUNAKAN ALGORITMA *ELLIPTIC CURVE CRYPTOGRAPHY*

disetujui dan disahkan oleh pembimbing:

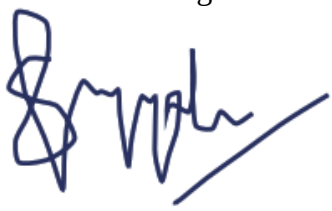
Pembimbing I



Dra. Rini Marwati, M.Si.

NIP. 196606251990012001

Pembimbing II

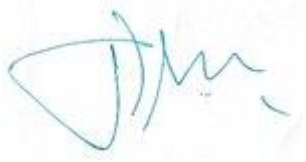


Ririn Sispiyati, S.Si., M.Si.

NIP.198106282005012001

Mengetahui,

Ketua Departemen Pendidikan Matematika,



Dr. H. Dadang Juandi, M.Si.

NIP. 196401171992021001

ABSTRAK

Kriptografi berperan penting pada era digital dalam mengamankan data dari peretas. Seiring berkembangnya teknologi, data yang dapat diamankan menggunakan kriptografi semakin luas, salah satunya adalah mengamankan gambar menggunakan kriptografi visual. Kriptografi visual merupakan kriptosistem yang memecah suatu gambar menjadi beberapa bagian dan hanya dapat dipecahkan jika memiliki semua bagian dari gambar tersebut. Jenis kriptografi lain yang dapat digunakan dalam mengamankan data adalah *elliptic curve cryptography* (ECC). ECC menggunakan suatu lapangan atas bilangan prima yang berisi titik-titik pada kurva eliptik sebagai teknik pengamanan datanya. Dalam penelitian ini dilakukan pengembangan kriptosistem dengan menggabungkan kriptografi visual dan ECC serta implementasinya dalam mengkonstruksi program aplikasi komputer menggunakan MATLAB R2014a. Pengembangan kriptografi visual menggunakan *Elliptic Curve Cryptography* dapat mempersulit kriptanalisis karena harus meretas dua algoritma dan tidak akan bisa diretas jika hanya memperoleh salah satu *share image*.

Kata Kunci: Kriptografi, Kriptografi Visual, *Elliptic Curve Cryptography*.

ABSTRACT

Cryptography held an important role in the digital era for securing data from hackers. As technology develops, types of data that can be secured using cryptography is expanding, one of which is securing images using visual cryptography. Visual cryptography is a cryptosystem that splits an image into parts and can only be solved if it has all parts of the image. Another type of cryptography that can be used to secure data is Elliptic Curve Cryptography (ECC). ECC uses a field of prime numbers consists of points on the elliptic curve as a technique to secure data. In this research, a cryptosystem development was carried out by visual cryptography combined with ECC and its implementation in constructing a computer application program using MATLAB R2014a. The development of visual cryptography using Elliptic Curve Cryptography can complicate cryptanalysis because it has two algorithms and cannot be hacked if only one share image was obtained.

Keywords: *Cryptography, Visual Cryptography, Elliptic Curve Cryptography*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR PUSTAKA

Artin, M. (1991). *Algebra*. New Jersey: Prentice Hall.

Azizah, H. N. (2019). *Penggabungan Modifikasi Hill Cipher dan Elliptic Curve Cryptography untuk Meningkatkan Keamanan Pesan*. Bandung: Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam, Unversitas Pendidikan Indonesia.

Durbin, J. R. (2009). *Modern Algebra*. Austin: John Wiley & Sons, Inc.

Herstein, I. N. (1975). *Topics in Algebra*. Chicago: John Wiley & Sons.

Hou, Young-Chang. (2002). *Visual Cryptography for Color Images*. Jung Li: Department of Information Management, National Central University.

Koblitz, N. (1984) Introduction to Elliptic Curves and Modular Forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York.

Kumar, D. S., Suneetha CH., & Chandrasekhar, A. (2012). *Encryption of Data Using Elliptic Curve Over Finite Fields*. International Journal of Distributed and Parallel System (IJDPS), 3 (1), hlm. 301-308.

Miller V.S. (1986). Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology — CRYPTO ’85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

Munir, R. (2010). *Matematika Diskrit* (3rd ed.). Bandung: Informatika Bandung.

Munthe, A. R., Ratnadewi. (2014). *Kriptografi Visual Pada Citra Berwarna Menggunakan Metode Kombinasi Perluasan Warna Red, Green dan Blue*. Bandung: Jurusan Teknik Elektro, Universitas Kristen Maranatha.

Naor, M., & Shamir, A. (1995). *Visual Cryptography*. Advances in Cryptology Vol. 950.

Ratnadewi. (2018). *Visual Cryptography with RSA Algorithm for Color Image*. Bandung: Department of Electrical Engineering, Universitas Kristen Maranatha.

Shankar, K., Devika, G., Ilayaraja, M. (2017). *Scheme based on Boolean Operations ad Elliptic Curve Cryptography*. Nadu: School of Computing, Kalasalingam University.

Siahaan, Andysah P. U. (2016) *RC4 Technique in Visual Cryptography RGB Image Encryption*. Medan: Faculty of Computer Science, Universitas Pembangunan Panca Budi.

Stinson, R. D. (2006). *Cryptography Theory and Practice*. Ontario: Chapman & Hall/CRC.