

# 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) MENGUNAKAN 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

© Della Annisa Zahra 2020  
Universitas Pendidikan Indonesia  
Agustus 2020

Hak Cipta dilindungi undang-undang.  
Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian,  
dengan dicetak ulang, difoto kopi, atau cara lainnya tanpa ijin dari penulis.

**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

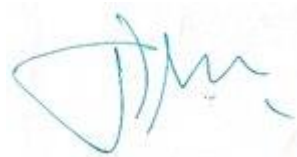


**Ririn Sispiyati, S.Si., M.Si.**

**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

LEMBAR PERNYATAAN .....	i
KATA PENGANTAR .....	ii
UCAPAN TERIMAKASIH .....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i> .....	v
DAFTAR ISI .....	vi
DAFTAR TABEL .....	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN .....	x
BAB I PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	2
1.3. Tujuan Penelitian .....	2
1.4. Batasan Masalah.....	3
1.5. Manfaat Penelitian .....	3
1.6. Sistematika Penulisan.....	3
BAB II LANDASAN TEORI.....	4
2.1. Grup.....	4
2.1.1. Grup Berhingga.....	4
2.1.2. Grup Siklik .....	4
2.2. Ring .....	5
2.3. Lapangan.....	5
2.4. <i>Discrete Logarithm Problem</i> .....	5
2.5. <i>Quadratic Residue</i> .....	6
2.6. Kriteria Euler.....	6
2.7. Kurva Eliptik pada $\mathbb{R}$ .....	6
2.8. Kurva Eliptik pada Lapangan $\mathbb{Z}_p$ .....	7
2.8.1. Logaritma Diskrit pada Kurva Eliptik.....	9
2.9. Kriptografi.....	9
2.9.1. Kriptografi Visual .....	10

2.9.2. Kriptografi Visual Perluasan RGB.....	11
2.9.3. Kriptografi Asimetris .....	13
2.9.4. <i>Elliptic Curve Cryptography</i> (ECC) .....	13
2.10. MATLAB.....	15
BAB III METODOLOGI PENELITIAN .....	17
3.1. Identifikasi Masalah .....	17
3.2. Model Dasar .....	17
3.2.1. Kriptografi Visual pada Gambar Berwarna RGB.....	18
3.2.2. <i>Elliptic Curve Cryptography</i> .....	18
3.3. Pengembangan Kriptografi Visual Menggunakan ECC .....	19
3.3.1. Proses Pembangkitan Kunci .....	21
3.3.2. Enkripsi.....	21
3.3.3. Dekripsi .....	22
3.4. Konstruksi Program Komputer .....	26
3.4.1. Input dan Output Program .....	26
3.4.2. Rancangan Tampilan .....	26
3.4.3. Algoritma.....	27
3.5. Validasi .....	32
BAB IV HASIL DAN PEMBAHASAN.....	33
4.1. Program Kriptografi Visual Menggunakan ECC.....	33
4.2. Validasi Program dengan Contoh .....	34
BAB V KESIMPULAN DAN SARAN .....	38
5.1. Kesimpulan.....	38
5.2. Saran .....	38
DAFTAR PUSTAKA.....	40
LAMPIRAN .....	42

## DAFTAR TABEL

Tabel 2.1. Analisa RGB pada Suatu Pixel .....	12
Tabel 2.2. Tabel Konversi Simbol ke Titik Kurva.....	14
Tabel 2.3. Titik Kurva $E: y^2 = x^3 + x + 6 \pmod{11}$ .....	15
Tabel 3.1. Tabel Konversi.....	23
Tabel 3.2. Hasil Konversi Warna.....	23
Tabel 3.3. Hasil Enkripsi Foto .....	24
Tabel 3.4. Hasil Dekripsi Foto .....	25



## DAFTAR GAMBAR

Gambar 2.1. Kurva Eliptik $y^2 = x^3 - 5x + 2$ .....	7
Gambar 2.2. Titik pada Kurva Eliptik $y^2 = x^3 + 4x + 7 \pmod{23}$ .....	9
Gambar 2.3. Matriks Representasi Warna Pixel .....	10
Gambar 2.4. Contoh Rekonstruksi Pixel Menggunakan OR .....	13
Gambar 3.1. Skema Alur Kriptografi Visual Menggunakan ECC.....	20
Gambar 3.2. Contoh Foto.....	22
Gambar 3.3. Hasil <i>Share</i> .....	25
Gambar 3.4. Rancangan Aplikasi Pembangkit Kunci ECC.....	26
Gambar 3.5. Rancangan Aplikasi Enkripsi Foto.....	27
Gambar 3.6. Rancangan Aplikasi Dekripsi Foto .....	27
Gambar 3.7. Diagram Alir Algoritma Pembentukan Kunci .....	28
Gambar 3.8. Diagram Alir Algoritma Pembentukan Tabel Konversi .....	29
Gambar 3.9. Diagram Alir Algoritma Enkripsi .....	30
Gambar 3.10. Diagram Alir Algoritma Dekripsi .....	31
Gambar 4.1. Tampilan Program Pembangkitan Kunci ECC .....	33
Gambar 4.2. Tampilan Program Enkripsi Foto.....	34
Gambar 4.3. Tampilan Program Dekripsi Foto.....	34
Gambar 4.4. Contoh Penggunaan Program Pembangkit Kunci.....	35
Gambar 4.5. Contoh Penggunaan Program Enkripsi Foto.....	36
Gambar 4.6. Hasil <i>Share Image</i> .....	36
Gambar 4.7. Contoh Penggunaan Program Dekripsi Foto.....	37

## DAFTAR LAMPIRAN

Lampiran 1. <i>Listing</i> Kode Program.....	41
--	----

## 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, Universitas 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](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.