

SKRIPSI

**KRIPTOGRAFI CITRA DIGITAL MENGGUNAKAN ARNOLD *CAT MAP*
DAN KURVA ELIPTIK PADA LAPANGAN BERHINGGA PRIMA**

*DIGITAL IMAGE CRYPTOGRAPHY BY USING ARNOLD CAT MAP AND
ELLIPTIC CURVE OF PRIME FINITE FIELD*



RAISA FATIMATHUZ ZAHRA

24010119130048

**DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
SEMARANG**

2023

SKRIPSI

**KRIPTOGRAFI CITRA DIGITAL MENGGUNAKAN ARNOLD *CAT MAP*
DAN KURVA ELIPTIK PADA LAPANGAN BERHINGGA PRIMA**

*DIGITAL IMAGE CRYPTOGRAPHY BY USING ARNOLD CAT MAP AND
ELLIPTIC CURVE OF PRIME FINITE FIELD*

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Sarjana
Matematika (S.Mat.)



RAISA FATIMATHUZ ZAHRA

24010119130048

**DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
SEMARANG**

2023

HALAMAN PENGESAHAN

SKRIPSI

**KRIPTOGRAFI CITRA DIGITAL MENGGUNAKAN ARNOLD *CAT MAP*
DAN KURVA ELIPTIK PADA LAPANGAN BERHINGGA PRIMA**

Telah dipersiapkan dan diusulkan oleh:

RAISA FATIMATHUZ ZAHRA

24010119130048

Telah dipertahankan di depan Tim Penguji

pada tanggal 10 Oktober 2023

Susunan Tim Penguji

Pembimbing II/Penguji,

Penguji


Prof. Dr. Widowati, S.Si., M.Si.
NIP. 196902141994032002


Solikhin S.Si., M.Sc.
NIP. 198506302012121001

Mengetahui,
Ketia Departemen Matematika,

Pembimbing I/Penguji,


Dr. Susilo Hartono, S.Si., M.Si.
NIP. 197410142000121001


Dr. Nikken Prima Puspita S.Si., M.Sc.
NIP. 198604132009122007

HALAMAN PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali yang tertulis dan diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Semarang, Oktober 2023

Raisa Fatimathuz Zahra

HALAMAN PERSEMBAHAN

Kupersembahkan karya ini untuk:

Diriku, Ayah, Ibu, kedua adik dan Sahabat

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadiran Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Skripsi yang berjudul “**Kriptografi Citra Digital Menggunakan Arnold Cat Map Dan Kurva Eliptik Pada Lapangan Prima**”. Skripsi ini disusun sebagai persyaratan untuk memperoleh gelar Sarjana Strata Satu (S1) pada Departemen Matematika, Fakultas Sains dan Matematika, Universitas Diponegoro, Semarang.

Tanpa adanya dukungan dan bantuan dari berbagai pihak, Skripsi ini tidak akan dapat terselesaikan dengan baik. Oleh karena itu, penulis ingin mengucapkan terima kasih dan rasa hormat kepada:

1. Dr. Susilo Hariyanto, S.Si., M.Si. selaku Ketua Departemen Matematika, Fakultas Sains dan Matematika, Universitas Diponegoro.
2. Dr. Nikken Prima Puspita S.Si., M.Sc. selaku Dosen Pembimbing 1 yang telah memberikan bimbingan, pengarahan dan motivasi kepada penulis dalam penyusunan dari awal hingga akhir penyusunan Skripsi ini.
3. Prof. Dr. Widowati, S.Si., M.Si. selaku Dosen Pembimbing 2 yang telah meluangkan waktu dan memberikan bimbingan serta pengarahan kepada penulis dalam penyusunan Skripsi ini.
4. Semua pihak yang telah memberikan bantuan, bimbingan, serta membantu kelancaran penyusunan tugas akhir ini, yang tidak dapat disebutkan.

Penulis menyadari bahwa tugas akhir ini masih jauh dari kata sempurna dan masih banyak yang harus dibenahi. Semoga tugas akhir ini bermanfaat bagi pembaca.

Semarang, Oktober 2023

Raisa Fatimathuz Zahra

DAFTAR ISI

HALAMAN PENGESAHAN.....	iii
HALAMAN PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR.....	vi
DAFTAR ISI	vii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR ARTI LAMBANG	xi
ABSTRAK	xii
ABSTRACT.....	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan masalah.....	2
1.3 Tujuan dan Manfaat Penelitian.....	2
1.3.1 Tujuan Penelitian.....	2
1.3.2 Manfaat Penelitian	3
1.4 Sistematika Penulisan.....	3
BAB II LANDASAN TEORI	5
2.1 Struktur Aljabar	5
2.1.1 Grup	5
2.1.2 Ring.....	9
2.1.3 Lapangan dan Daerah Integral	13
2.2 Teori Bilangan	16
2.2.1 Himpunan Bilangan Bulat.....	16
2.2.2 Aritmatika Modulo.....	19
2.2.3 Bilangan Prima.....	21
2.3 Matriks.....	23
2.4 Citra Digital.....	25
2.5 Kriptografi.....	27

2.5.1	Sejarah Kriptografi.....	28
2.5.2	Kriptografi Simetris dan Asimetris	30
BAB III METODOLOGI PENELITIAN.....		31
3.1	Bahan dan Alat Penelitian	31
3.2	Prosedur Kerja	31
BAB IV PEMBAHASAN.....		33
4.1	Arnold <i>Cat Map</i>	33
4.2	Lapangan Berhingga Prima $GF(p)$	37
4.3	Kriptografi Kurva Eliptik atas Lapangan Berhingga Prima $GF(p)$	40
4.4	Penerapan Kriptografi <i>Arnold Cat Map</i> dan Kurva Eliptik.....	52
4.4.1	Pembentukan Kunci	52
4.4.2	Algoritma Enkripsi.....	53
4.4.3	Algoritma Dekripsi.....	54
4.4.4	Simulasi Kriptografi Metode Arnold Cat Map dan Kurva Eliptik..	54
BAB V KESIMPULAN.....		72
DAFTAR PUSTAKA		73

DAFTAR TABEL

Tabel 2. 1 Penjumlahan " \oplus " pada himpunan D	6
Tabel 2. 2 Operasi perkalian " \odot " pada himpunan D	10
Tabel 2. 3 Perkalian Modulo 12 pada himpunan \mathbb{Z}_{12}	12
Tabel 2. 4 Operasi perkalian di \mathbb{Z}_7	20
Tabel 4. 1 Operasi penjumlahan di $GF(5)$	38
Tabel 4. 2 Operasi penjumlahan di $GF(5)$	38
Tabel 4. 3 Mencari himpunan elemen residu kuadrat di \mathbb{Z}_{11}	49
Tabel 4. 4 Mencari elemen residu kuadrat modulo 5	50
Tabel 4. 5 Mencari nilai $y^2 = x^3 + 2x + 1 \text{ mod } 5$	50
Tabel 4. 6 Mencari pasangan terurut $E_5(2,1)$	51
Tabel 4. 7 Hasil Konversi Nilai RGB ke Titik Kurva Eliptik	59
Tabel 4. 8 Hasil Konversi Titik Kurva Eliptik ke Nilai RGB	62
Tabel 4. 9 Hasil Konversi Nilai RGB ke Titik Kurva Eliptik	64
Tabel 4. 10 Hasil Konversi Titik Kurva Eliptik ke Nilai RGB	68

DAFTAR GAMBAR

Gambar 2. 1 Representasi Citra Digital Berukuran $M \times N$	26
Gambar 2. 2 Tingkat Keabuan dari Hitam ke Putih	26
Gambar 3. 1 Diagram alir enkripsi pada citra digital	32
Gambar 4. 1 Gambar Awal Ukuran 2×2	35
Gambar 4. 2 Gambar Hasil Pengacakan Posisi Piksel.....	36
Gambar 4. 3 Hasil Mengembalikan Posisi Piksel Gambar.....	37
Gambar 4. 4 Kurva eliptik $y^2 = x^3 + 1$ di \mathbb{R}	41
Gambar 4. 5 Ilustrasi Penjumlahan $P + Q = R$	43
Gambar 4. 6 Ilustrasi Penjumlahan $P + P = R$	45
Gambar 4. 7 Ilustrasi Penjumlahan $P + (-P) = O$	46
Gambar 4. 8 Citra Digital 4×4 piksel.....	55
Gambar 4. 9 Citra Digital Hasil Pengacakan Piksel.....	57
Gambar 4. 10 Citra Digital Hasil Enkripsi	63
Gambar 4. 11 Citra Digital Hasil Dekripsi	68
Gambar 4. 12 Citra Digital Hasil dari Pengembalian Posisi Piksel.....	71

DAFTAR ARTI LAMBANG

\mathbb{Z}	: Himpunan semua bilangan bulat
\mathbb{Z}_n	: Himpunan semua bilangan modulo n
$x \in X$: elemen x anggota himpunan A
$+_n$: Operasi penjumlahan modulo n
\cdot_n	: Operasi perkalian modulo n
1_R	: Elemen satuan di ring R
L	: Tingkat keabuan dari citra digital
k	: Besaran bit
(x, y)	: Posisi piksel
$R(x, y)$: intensitas warna merah pada piksel (x, y)
$G(x, y)$: intensitas warna hijau pada piksel (x, y)
$B(x, y)$: intensitas warna biru pada piksel (x, y)
(x', y')	: Posisi baru piksel
$\det(A)$: determinan matriks A
p	: Bilangan prima
GF	: Galois <i>field</i> / lapangan Galois
$E_p(a, b)$: Himpunan titik pada kurva eliptik $y^2 = x^3 + ax + b \pmod{p}$
QR_n	: Himpunan elemen residu kuadrat modulo n
K_p	: Kunci Privat
K_b	: Kunci Publik
G	: Titik Basis
P	: <i>Plain Text</i> / plainteks
C	: <i>chipher Text</i> / cipherteks

ABSTRAK

KRIPTOGRAFI CITRA DIGITAL MENGGUNAKAN ARNOLD *CAT MAP* DAN KURVA ELIPTIK PADA LAPANGAN BERHINGGA PRIMA

Oleh

RAISA FATIMATHUZ ZAHRA

24010119130048

Citra digital adalah salah satu media teknologi yang sering digunakan sehingga rentan dimanipulasi. Pada citra digital diperlukan sebuah skema yang membuat data tersebut hanya bisa diakses oleh orang yang dituju. Kriptografi dapat digunakan untuk menjaga keaslian dan keamanan dari citra digital. Oleh karena itu, dirancang algoritma enkripsi citra digital menggunakan metode Arnold *Cat Map* dan kurva eliptik pada lapangan berhingga prima. Penggunaan algoritma Arnold *Cat Map* diperlukan untuk memperkuat daya tahan terhadap pembobolan pesan karena posisi piksel telah diacak dengan pola yang tidak mudah diprediksi. Proses enkripsi dan dekripsi citra digital digunakan kurva eliptik pada lapangan berhingga prima. Pada simulasi yang telah dilakukan pada skripsi ini diperoleh bahwa algoritma dari metode Arnold *Cat Map* dan kurva eliptik pada lapangan berhingga prima memiliki keamanan yang baik dalam menjaga kerahasiaan informasi citra digital karena pesan asli sangat berbeda dengan pesan hasil enkripsi.

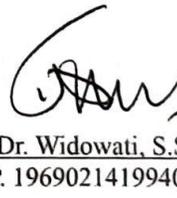
Kata kunci : Arnold *Cat Map*, kurva eliptik, kriptografi, lapangan Galois prima

Pembimbing I,



Dr. Nikken Prima Puspita S.Si., M.Sc.
NIP. 198604132009122007

Pembimbing II,



Prof. Dr. Widowati, S.Si., M.Si.
NIP. 196902141994032002

ABSTRACT

DIGITAL IMAGE CRYPTOGRAPHY BY USING ARNOLD CAT MAP AND ELLIPTIC CURVE OF PRIME FINITE FIELD

By

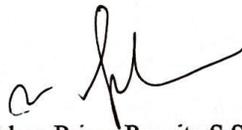
RAISA FATIMATHUZ ZAHRA

24010119130048

Digital images are a technological medium that is frequently used and therefore vulnerable to manipulation. Digital images require a scheme that makes the data only accessible to the recipient. Cryptographic techniques can be used to ensure the authenticity and security of digital images. Therefore, a digital image encryption algorithm was designed using the Arnold Cat Map method and elliptic curves in a prime finite field. The use of the Arnold Cat Map algorithm is necessary to strengthen resistance to message hacking because pixel positions have been randomized in a pattern that is not easily predictable. The digital image encryption and decryption process uses an elliptic curve on a prime Galois field. In the simulations carried out on this script, it was found that the algorithm of the Arnold Cat Map method and elliptic curves in prime finite fields has good security in maintaining the confidentiality of digital image information because the original message is very different from the encrypted message.

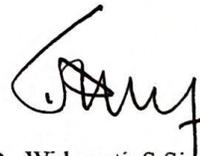
Kata kunci : Arnold *Cat Map*, elliptic curves, cryptography, prime Galois field

Pembimbing I,



Dr. Nikken Prima Puspita S.Si., M.Sc.
NIP. 198604132009122007

Pembimbing II,



Prof. Dr. Widowati, S.Si., M.Si.
NIP. 196902141994032002