

**IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY*
(ECC) DAN STEGANOGRAFI *SPREAD SPECTRUM* PADA
PENGAMANAN PESAN KE DALAM GAMBAR**

SKRIPSI

Diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar

Sarjana Matematika



Oleh:

Muhammad Daud

NIM: 1904812

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

2023

**IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY*
(ECC) DAN STEGANOGRAFI *SPREAD SPECTRUM* PADA
PENGAMANAN PESAN KE DALAM GAMBAR**

Oleh:

Muhammad Daud

NIM 1904812

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

© Muhammad Daud 2023

Universitas Pendidikan Indonesia

Agustus 2023

Hak cipta dilindungi undang-undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian, dengan dicetak ulang,
fotokopi, atau cara lainnya tanpa izin dari penulis

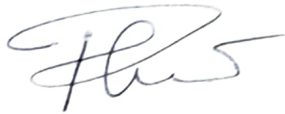
LEMBAR PENGESAHAN

MUHAMMAD DAUD

**IMPLEMENTASI KRIPTOGRAFI *ELLIPTIC CURVE CRYPTOGRAPHY* (ECC) DAN
STEGANOGRAFI *SPREAD SPRECTRUM* PADA PENGAMANAN PESAN KE DALAM
GAMBAR**

Disetujui dan disahkan oleh pembimbing:

Pembimbing I



Dra. Hj. Rini Marwati, M.Si.

NIP. 196606251990012001

Pembimbing II



Dr. Sumanang Muhtar Gozali, M.Si.

NIP. 197411242005011001

Mengetahui

Ketua Program Studi Matematika



Dr. Kartika Yulianti, S.Pd., M.Si.

NIP. 198207282005012001

SURAT PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul “Implementasi Kriptografi *Elliptic Curve Cryptography* (ECC) dan Steganografi *Spread Spectrum* pada Pengamanan Pesan ke dalam Gambar” ini beserta seluruh isinya adalah benar-benar karya saya sendiri, kecuali kutipan-kutipan dari ringkasan yang semuanya telah saya jelaskan sumbernya. Apabila dikemudian hari ditemukan adanya pelanggaran, saya bersedia menanggung resiko atau sanksi yang dijatuhkan kepada saya.

Bandung, 29 Juli 2023

Yang membuat pernyataan,



Muhammad Daud

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, karena berkat rahmat dan karunia-Nya penulis dapat menyelesaikan skripsi yang berjudul “Implementasi Kriptografi *Elliptic Curve Cryptography* (ECC) dan Steganografi *Spread Spectrum* pada Pengamanan Pesan ke dalam Gambar” sebagai salah satu syarat memperoleh gelar Sarjana Matematika di Universitas Pendidikan Indonesia (UPI).

Penulis menyadari bahwa masih terdapat kekurangan di penulisan skripsi ini. Oleh karena itu kritik dan saran yang membangun sangat diperlukan guna menyempurnakan dan mengembangkan skripsi ini. Penulis berharap skripsi ini dapat bermanfaat bagi pembaca, khususnya yang sedang mendalami kriptografi ECC dan steganografi *Spread Spectrum*.

Bandung, 29 Juli 2023

Penulis

UCAPAN TERIMAKASIH

Penulis menyadari bahwa selama penulisan skripsi terdapat pihak yang secara langsung maupun tidak langsung telah memberikan bantuan, doa, dan semangat. Oleh karena itu, penulis ingin menyampaikan terimakasih kepada:

1. Ibu Dra. Hj. Rini Marwati, M.Si. selaku dosen Pembimbing I yang telah mengajarkan penulis dengan penuh kesabaran mengenai topik yang penulis bahas dalam skripsi ini.
2. Bapak Dr. Sumanang Muhtar Gozali, M.Si. selaku dosen Pembimbing II yang telah memberikan arahan dan bimbingan dari awal hingga akhir penulisan skripsi ini.
3. Ibu Hj. Entit Puspita, S.Pd., M.Si. selaku dosen pembimbing akademik yang telah membina penulis selama menjalani perkuliahan di UPI.
4. Kedua orang tua yang telah mendoakan dan mendukung agar skripsi ini dapat diselesaikan tepat waktu.
5. Rekan-rekan mahasiswa Matematika UPI 2019 yang juga telah memberikan motivasi dan dukungannya, serta menemani penulis belajar selama masa perkuliahan.
6. Pihak lainnya yang tidak bisa disebutkan satu persatu yang telah membantu penulis dalam perkuliahan maupun penyelesaian skripsi ini.

Penulis

ABSTRAK

Kemajuan teknologi membuat seseorang menjadi lebih mudah untuk berkomunikasi. Namun seringkali pesan yang dikirim diretas oleh pihak yang tidak berhak. Oleh karena itu dibutuhkan suatu sistem keamanan yang dapat mencegah peretasan tersebut oleh pihak yang tidak berhak. Media komunikasi yang digunakan saat ini ada berbagai jenis, antara lain berbentuk *file* teks dan juga *file* gambar. Cara untuk mengamankan data antara lain dapat menggunakan kriptografi dan juga steganografi. Penelitian ini mengimplementasikan dan mengonstruksi program aplikasi untuk penyamaran pesan menggunakan kriptografi *Elliptic Curve Cryptography* (ECC) dan steganografi *Spread Spectrum*. Pesan yang telah dienkripsi menggunakan kriptografi ECC disembunyikan ke dalam gambar menggunakan steganografi *Spread Spectrum*. Program aplikasi kriptografi ECC dan steganografi *Spread Spectrum* pada pengamanan pesan ke dalam gambar akan dikonstruksi menggunakan bahasa pemrograman *Python*. Hasil penyisipan pesan yang telah dienkripsi ke dalam gambar tidak menimbulkan perubahan yang signifikan pada gambar sehingga pesan dapat disembunyikan dengan baik tanpa menimbulkan kecurigaan.

Kata Kunci: Kriptografi, *Elliptic Curve Cryptography*, Steganografi, *Spread Spectrum*

ABSTRACT

Advances in technology make it easier for people to communicating. But often the messages sent are hacked by unauthorized parties. Therefore, there is a need for a security system that can prevent the message from being hacked by unauthorized parties. There are various types of communication media used today, including text files and image files. Ways to secure data include cryptography and steganography. This research implements and constructs an application program to secure messages using Elliptic Curve Cryptography (ECC) and Spread Spectrum steganography. Messages that have been encrypted using ECC cryptography are hidden into images using Spread Spectrum steganography. The application program of ECC cryptography and Spread Spectrum steganography on securing messages into images will be constructed using the Python programming language. The results of inserting a message that has been encrypted into the image do not cause significant changes in the image so the message can be hidden properly without causing suspicion.

Keywords: *Cryptography, Elliptic Curve Cryptography, Steganography, Spread Spectrum*

DAFTAR ISI

LEMBAR PENGESAHAN	i
SURAT PERNYATAAN	ii
KATA PENGANTAR	iii
UCAPAN TERIMAKASIH	iv
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	3
1.4 Manfaat Penelitian	4
1.5 Batasan Masalah	4
BAB II LANDASAN TEORI	5
2.1 Teori Aljabar	5
2.1.1 Grup	5
2.1.2 Ring	6
2.1.3 Lapangan	6
2.2 Kriptografi (Stinson, 2006)	6
2.2.1 Istilah dalam Kriptografi	7

2.2.2	Tujuan Kriptografi	7
2.3	Kurva Eliptik.....	8
2.3.1	Logaritma Diskrit	8
2.3.2	Logaritma Diskrit pada Kurva Eliptik	8
2.3.3	<i>Quadratic Residue</i>	8
2.3.4	Kriteria Euler	9
2.3.5	Kurva Eliptik pada \mathbb{R}	9
2.3.6	Kurva Eliptik pada Lapangan \mathbb{Z}_p	10
2.4	<i>Elliptic Curve Cryptography</i> (ECC).....	12
2.4.1	Konversi Pesan Asli pada Titik di Kurva Eliptik	12
2.4.2	Enkripsi.....	13
2.4.3	Dekripsi.....	13
2.5	Steganografi.....	14
2.5.1	Istilah dalam Steganografi	15
2.5.2	Prinsip Kerja Steganografi.....	15
2.6	Metode <i>Spread Spectrum</i>	16
2.7	Data Teks	22
2.8	Bahasa Pemrograman Python	22
BAB III METODE PENELITIAN		23
3.1	Identifikasi Masalah	23
3.2	Model Dasar	23
3.2.1	<i>Elliptic Curve Cryptography</i>	24
3.2.2	<i>Spread Spectrum</i>	25
3.3	Pengembangan Model Dasar	25

3.4	Konstruksi Program Aplikasi	27
3.4.1	Input dan Output	27
3.4.2	Algoritma Deskriptif.....	27
3.4.3	Rancangan Tampilan Program Aplikasi	27
3.4.4	<i>Library</i> Program.....	30
3.5	Proses Validasi	30
3.6	Pengambilan Kesimpulan	31
BAB IV	HASIL DAN PEMBAHASAN	32
4.1	Algoritma Kriptografi ECC dan Steganografi Spread Spectrum	32
4.1.1	Algoritma ECC pada Enkripsi Pesan	32
4.1.2	Algoritma <i>Spread Spectrum</i> pada <i>Embedding</i> Gambar	34
4.1.3	Algoritma <i>Spread Spectrum</i> pada Ekstraksi Gambar.....	37
4.1.4	Algoritma ECC pada Dekripsi Cipherteks.....	38
4.2	Program Kriptografi ECC dan Steganografi Spread Spectrum	38
4.3	Validasi.....	42
BAB V	KESIMPULAN DAN SARAN	52
5.1	Kesimpulan.....	52
5.2	Saran	52
DAFTAR PUSTAKA.....		54
Lampiran.....		57

DAFTAR GAMBAR

Gambar 2.1 Kurva Eliptik $y^2 = x^3 - 7x + 4$	10
Gambar 2.2 Titik-titik pada Kurva Eliptik $y^2 = x^3 - 7x + 4 \bmod 71$	11
Gambar 2.3 Skema Proses <i>Embedding</i> Pesan.....	17
Gambar 2.4 Skema Proses Ekstraksi Pesan	17
Gambar 3.1 Algoritma Pembangkitan Kunci Kriptografi ECC	24
Gambar 3.2 Skema Kriptografi ECC	24
Gambar 3.3 Skema Steganografi Spread Spectrum	25
Gambar 3.4 Skema Pengembangan Model.....	26
Gambar 3.5 Proses Pembangkitan Kunci ECC	28
Gambar 3.6 Proses Enkripsi	28
Gambar 3.7 Proses Embedding	29
Gambar 3.8 Proses Ekstraksi.....	29
Gambar 3.9 Proses Dekripsi.....	30
Gambar 4.1 Skema Pengembangan Algoritma Kriptografi ECC dan Steganografi Spread Spectrum	32
Gambar 4.2 Pseudocode Pembangkitan Kunci ECC	33
Gambar 4.3 Pseudocode Proses Enkripsi	34
Gambar 4.4 Pseudocode Pembangkitan Kunci Spread Spectrum	35
Gambar 4.5 Pseudocode Embedding Cipherteks ke Dalam Gambar	36
Gambar 4.6 Pseudocode Proses Ekstraksi.....	37
Gambar 4.7 Pseudocode Dekripsi Cipherteks.....	38
Gambar 4.8 Tampilan Pembangkitan Kunci ECC	39

Gambar 4.9 Tampilan Proses Enkripsi.....	39
Gambar 4.10 Tampilan Proses Embedding.....	40
Gambar 4.11 Tampilan Proses Ekstraksi	41
Gambar 4.12 Tampilan Proses Dekripsi.....	41
Gambar 4.13 Tampilan Pembangkitan Kunci ECC.....	42
Gambar 4.14 Tampilan Proses Enkripsi.....	43
Gambar 4.15 Tampilan Proses Embedding.....	44
Gambar 4.16 Tampilan Proses Ekstraksi	48
Gambar 4.17 Tampilan Proses Dekripsi.....	51

DAFTAR TABEL

Tabel 2.1 Tabel Konversi Simbol ke Titik Kurva	13
Tabel 2.2 Proses Pencarian Titik pada Kurva	14
Tabel 2.3 Konversi Pesan ke Biner	17
Tabel 2.4 Konversi Pseudonoise ke Biner	18
Tabel 2.5 Pembangkitan Kunci dengan Metode LCG.....	20
Tabel 2.6 Proses embedding.....	21
Tabel 4.1 Proses Pencarian Titik pada Kurva	43
Tabel 4.2 Perhitungan Manual Proses Enkripsi	44
Tabel 4.3 Konversi Karakter ke Biner	45
Tabel 4.4 Proses Penyisipan	47
Tabel 4.5 Perhitungan Manual Proses Ekstraksi.....	49
Tabel 4.6 Konversi Biner ke Karakter	50
Tabel 4.7 Perhitungan Manual Proses Dekripsi	51

DAFTAR LAMPIRAN

Lampiran 1 Kode Pembangkit Kunci ECC.....	49
Lampiran 2 Kode Enkripsi	49
Lampiran 3 Kode Dekripsi.....	49
Lampiran 4 Kode Pseudonoise	49
Lampiran 5 Kode Embedding	49
Lampiran 6 Kode Ekstraksi.....	49

DAFTAR PUSTAKA

- Cahyani, A. D. (2022). Penyamaran Teks dengan Skema *Hybrid* Menggunakan Algoritma Enigma dan Algoritma Elgamal. Skripsi Sarjana. Universitas Pendidikan Indonesia.
- Handoyo, A. E., dkk. (2018). Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *Jurnal Teknologi dan Sistem Komputer*, 6(1).
- Herstein, I. N. (1975). *Topics in Algebra*. John Wiley and Sons Inc.
- Hikmah, A. N. (2020). Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey Vigenere Cipher* dan Algoritma *Elgamal*. Skripsi Sarjana. Universitas Pendidikan Indonesia.
- Gunawan, I., & Sumarmo. (2018). Penggunaan Algoritma Kriptografi Steganografi *Least Significant Bit* Untuk Pengamanan Pesan Teks dan Data Video 64. *Jurnal Sains Komputer & Informatika*, Vol.2, No.1, Maret 2018.
- Jaya, I. M. (2017). Implementasi Kriptografi Pengamanan Pesan Email Dengan Kombinasi Algoritma *Caesar Cipher* Dan *Vigenere Cipher*.
- Munir, R. (2019). *Kriptografi Edisi 2*. Bandung: Institut Teknologi Bandung.
- Naufal, M. F. (2021). Kriptografi Audio Menggunakan Transposisi dan *Affine Cipher* yang Dikembangkan dengan Algoritma *Blum Blum Shub*. Skripsi Sarjana. Universitas Pendidikan Indonesia.

- Noercholis, A., & Nugraha, Y. (2016). Pengamanan Data Teks Menggunakan Teknik Steganografi *Spread Spectrum* Berbasis Android. *Jurnal Antivirus*, 10(1), 1 Mei 2016.
- Pakereng, I. M. A. (2010). Perbandingan Steganografi Metode *Spread Spectrum* dan *Least Significant Bit (LSB)* Antara Waktu Proses dan Ukuran File Gambar. *Jurnal Informatika*, Vol 6, No 2, 2010.
- Putranto, A. (2009). Steganografi Melalui Media Gambar dengan Metode *Spread Spectrum*. Program Studi Teknik Informatika. Institut Teknologi Bandung.
- Ridho, A. (2022). Implementasi Enkripsi *Vigenere Cipher* dan *Reverse Cipher* Menggunakan Bahasa Pemrograman *Python*. *Jurnal Teknologi Informasi*, Vol 1, No 1. Mei 2022.
- Scheiner, B. (1996). *Applied Cryptography 2nd*. John Wiley and Sons.
- Septayuda, A., Hidayat, B., & Nuha, H. H. (2014). Analisis Steganografi Citra Digital Menggunakan Metode *Spread Spectrum* Berbasis Android. *E-Proceeding of Engineering : Vol.1, No.1 Desember 2014*.
- Sinaga, M. (2020). Implementasi Steganografi Menggunakan Metode *Spread Spectrum* dalam Pengamanan Data Teks pada Citra Digital. Skripsi Sarjana. Universitas Islam Negeri Sumatera Utara.
- Stinson, D. R. (2006). *Cryptography Theory and Practice 3rd Edition*. Chapman and Hall/CRC.
- Vembrina, Y. G. (2006). *Spread Spectrum Steganografi*. Program Studi Teknik Informatika. Institut Teknologi Bandung.

Yusuf, R. N., Furqan, M., & Sinaga, M. S. (2020). Implementasi Steganografi Menggunakan Metode *Spread Spectrum* Dalam Pengamanan Data Teks Pada Citra Digital. *Jurnal Sains Komputer & Informatika*, Vol.4, No.2, September 2020.

Zahra, D. A. (2020). Kriptografi Visual pada Gambar Berwarna (RGB) Menggunakan Algoritma *Elliptic Curve Cryptography*. Skripsi Sarjana. Universitas Pendidikan Indonesia.