BAB I
PENDAHULUAN

1.1. Latar Belakang

Kriptografi berasal dari bahasa Yunani, yaitu *kryptos* (tersembunyi) dan *graphein* (menulis), yang dapat diartikan sebagai keahlian dan ilmu dari cara-cara berkomunikasi dengan aman terhadap pihak ketiga (Munir, 2010). Kriptografi dapat digunakan untuk mengamankan informasi berupa teks maupun gambar. Untuk data berupa gambar, salah satu metode yang digunakan adalah kriptografi visual.

Kriptografi visual adalah salah satu teknik kriptografi dalam mengamankan data. Media yang digunakan dapat berupa gambar maupun video. Teknik ini diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1985. Langkah yang dilakukan untuk mengenkripsi data adalah dengan merekonstruksi data awal menjadi beberapa bagian, sedangkan untuk mendekripsinya dapat dilakukan dengan menggabungkan bagian-bagian hasil rekonstruksi sehingga memunculkan isi dari pesan aslinya. Dalam jurnalnya, Naor dan Shamir mengklaim bahwa data yang dienkripsi dijamin keamanannya, akan tetapi kunci yang digunakan untuk mengenkripsi tidak mudah diamankan. Oleh karena itu diperlukan peningkatan keamanan dari kriptografi visual.

Untuk kriptografi pada data berupa teks, terdapat dua algoritma kriptografi yang bisa digunakan yaitu algoritma simetris dan algoritma asimetris. Algoritma kriptografi asimetris dikenal juga dengan kriptografi kunci publik, di mana dibutuhkan dua buah kunci masing-masing untuk mengenkripsi pesan dan mendekripsi pesan. Salah satu metode kriptografi asimetris yang umum digunakan adalah kriptografi *Elliptical Curve Cryptography*.

Elliptical Curve Cryptography (ECC) adalah kriptografi asimetris yang dikembangkan oleh Victor Miller dan Neal Koblitz pada tahun 1985. ECC memanfaatkan permasalahan matematis kurva eliptik sebagai dasar keamanan pada algoritmanya. Keunggulan dari algoritma ECC adalah ukuran kunci yang lebih kecil daripada algoritma asimetris lainnya tetapi memiliki tingkat keamanan yang sama.

Menurut Andysah (2016) teknik enkripsi visual menggunakan RC4 meningkatkan keamanan kriptografi visual dengan memberikan tiga pilihan lapisan gambar yang akan dienkripsi. Ratnadewi (2018) mengajukan kriptografi visual pada gambar dengan format warna RGB yang digabungkan dengan algoritma RSA untuk masing-masing warna dasar. Hasil enkripsi berupa dua gambar dan hasil dekripsi dari dua gambar tersebut memberikan gambar asli dengan kualitas tinggi.

Penelitian mengenai penggabungan kriptografi visual dengan ECC telah dilakukan oleh Shankar, Devika, dan Ilayaraja (2017). Dalam jurnal tersebut disimpulkan bahwa hasil pengembangan kriptografi visual dengan menggunakan ECC untuk lebih dari satu *plain images* dengan teknik pemetaan menggunakan metode Koblitz untuk mengkonversi nilai RGB berhasil mempersingkat waktu komputasi, mempertahankan ukuran citra yang asli dengan yang sudah dienkripsi, menghasilkan *shared images* dengan jumlah yang sama dengan *plain images*, dan peningkatan keamanan pada *shared images*.

Berdasarkan uraian di atas, penulis mengkaji penggabungan kriptografi visual dengan kriptografi ECC untuk mengamankan gambar dengan mengkonversi warna dasar RGB menggunakan tabel yang dibentuk dari operasi perkalian pada titik generator. Hasil penggabungan tersebut dibuat program aplikasi komputer menggunakan bahasa pemrograman MATLAB.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, dirumuskan masalah sebagai berikut:

1. Bagaimana penggabungan algoritma ECC dengan kriptografi visual?
2. Bagaimana konstruksi program penggabungan algoritma ECC dengan kriptografi visual?

1.3. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengembangkan teknik kriptografi visual yang ditingkatkan menggunakan ECC.
2. Mengkonstruksi program enkripsi dan dekripsi untuk kriptografi visual yang ditingkatkan menggunakan ECC.

1.4. Batasan Masalah

Pada penelitian ini, pesan yang diamankan adalah gambar berwarna (RGB) dengan format *.JPEG atau *.JPG.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memberi kontribusi pada bidang matematika melalui pengembangan kriptografi visual menggunakan ECC sebagai metode baru dalam mengamankan data.
2. Mengembangkan sebuah aplikasi yang bertujuan untuk membantu proses pembangkitan kunci, enkripsi dan dekripsi pada kriptografi visual menggunakan ECC.

1.6. Sistematika Penulisan

Tulisan ini terdiri dari lima bab:

1. BAB I PENDAHULUAN

   Bab ini berisi tentang latar belakang penelitian, rumusan masalah, tujuan, manfaat, dan sistematika penulisan.
2. BAB II LANDASAN TEORI

   Bab ini berisi tentang teori-teori dasar yang berhubungan dan menunjang penelitian, di antaranya adalah logaritma diskrit dan kurva eliptik.
3. BAB III METODOLOGI PENELITIAN

   Bab ini menjelaskan langkah-langkah penelitian dan rumusan masalah, mengkaji model dasar, mengembangkan model dasar, mengkonstruksi program aplikasi dan validasi.
4. BAB IV PEMBAHASAN

   Bab ini memuat hasil penelitian tentang penggabungan kriptografi visual dengan ECC dan penerapannya dalam mengamankan suatu gambar berwarna. Bab ini juga memuat hasil konstruksi program.
5. BAB V KESIMPULAN DAN SARAN

   Bab ini membahas tentang kesimpulan dari hasil penelitian ini serta saran untuk pengembangan selanjutnya.