I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan internet di era modern telah memberikan dampak signifikan terhadap berbagai aspek kehidupan, salah satunya adalah penyimpanan dan pengelolaan data pribadi yang semakin mudah diakses dan digunakan dalam berbagai kegiatan, baik oleh pihak yang sah maupun pihak yang tidak bertanggung jawab (Betty Yel & M Nasution, 2022).

Menurut Badan Siber dan Sandi Negara (BSSN), peristiwa kebocoran data paling banyak terjadi di administrasi pemerintahan, yakni sebesar 55%. BSSN mencatat bahwa sebanyak 207 dugaan kebocoran data di Indonesia sepanjang tahun 2023 (Shanti, 2023). Pada tahun 2024, terdapat kejadian yang cukup menggemparkan, yaitu lumpuhnya server Pusat Data Nasional (PDN) akibat serangan *ransomware* oleh kelompok Brain Cipher. Peristiwa ini menyebabkan terganggunya layanan publik, termasuk imigrasi di bandara. Menurut Kementerian Komunikasi dan Informatika, total terdapat 282 instansi milik pemerintah yang datanya tersimpan di Pusat Data Nasional Sementara (PDNS) Surabaya terkena dampak serangan *ransomware*. Serangan ini mencangkup data dari kementerian, lembaga, serta pemerintah provinsi, kabupaten, dan kota. Kelompok Brain Cipher menggunakan varian *ransomware* LockBit 3.0 dan meminta uang tebusan sebesar USD 8 juta untuk membuka akses terhadap data yang terkunci (KOMINFO, 2024).

Salah satu jenis data penting yang rawan disalahgunakan adalah data pribadi yang terdapat pada Kartu Tanda Penduduk (KTP). KTP memuat informasi identitas seseorang seperti nama, tempat lahir, NIK, dan alamat, yang semuanya bersifat pribadi dan sensitif. Di antara informasi tersebut, data alamat menjadi bagian yang paling rentan, karena dapat digunakan untuk melacak keberadaan seseorang atau menjadi pintu masuk bagi tindak kejahatan berbasis identitas. Kebocoran data alamat berpotensi dimanfaatkan untuk kejahatan seperti penipuan, pencurian identitas, dan pelacakan lokasi pribadi. Oleh karena itu, perlindungan terhadap data alamat pada KTP menjadi sangat penting guna mencegah penyalahgunaan maupun kebocoran informasi pribadi (Suari & Sarjana, 2023). Salah satu pendekatan yang digunakan untuk mengamankan data adalah dengan menggunakan algoritma kriptografi. Kriptografi bertujuan untuk melindungi data dengan cara mengenkripsi data tersebut. Data yang telah dienkripsi akan menjadi tampak berbeda dengan aslinya, ini dilakukan dengan menggunakan algoritma matematika. Dengan demikian, seseorang yang tidak mengetahui kuncinya kemungkinan tidak akan dapat memahami isi data tersebut (KBBI, 2016).

Dalam algoritma kriptografi, dibutuhkan sebuah kunci untuk melakukan proses enkripsi dan dekripsi. Pada kriptografi terdapat dua jenis kunci utama yang dapat digunakan untuk mengenkripsi dan dekripsi sebuah data, yaitu kunci simetris dan kunci asimetris. Kunci simetris menggunakan kunci yang sama untuk enkripsi dan dekripsinya, sedangkan kunci asimetris menggunakan jenis kunci yang berbeda. Kriptografi asimetri pertama kali diperkenalkan pada pertengahan tahun 1970 –an oleh Whitfield Diffie dan Marthin Hellman (Safitri & Prihanto, 2019). Dalam kriptografi asimetris atau terkadang disebut juga kriptografi kunci-publik, digunakan sepasang kunci yang saling memiliki keterkaitan, di mana salah satunya kunci digunakan untuk proses enkripsi, sementara kunci lainnya digunakan dalam proses dekripsinya (Basri, 2016).

Beberapa algoritma kriptografi asimetris saat ini, seperti algoritma RSA, ElGamal dan Diffie-Hellman, menggunakan bilangan bulat yang sangat besar dalam proses enkripsi dan dekripsinya untuk mendapatkan tingkat keamanan yang lebih baik. Namun, hal ini dapat menyebabkan proses enkripsi dan dekripsinya menjadi lamban, serta mempengaruhi kapasitas penggunaan penyimpanan dan pengelolaan kunci serta pesan yang signifikan. Salah satu solusi pada permasalahan ini ialah menggunakan kriptografi yang berbasis pada daerah asal kurva eliptik, yang lebih efisien digunakan untuk mengamankan sebuah data.

Kriptografi kurva eliptik merupakan kriptografi berjenis kunci-publik yang lebih baru ditemukannya dan belum dianalisis dengan baik. Algoritma kriptografi kurva eliptik dirancang dan diajukan oleh Neal Koblitz dan Victor S. Miller pada tahun 1985. Pencipta kriptografi kurva eliptik mengklaim bahwa kriptografi kurva eliptik memberikan tingkat keamanan yang sama dengan algoritma kriptografi kunci-publik konvensional namun dengan ukuran kunci yang lebih pendek. Penemu kriptografi kurva eliptik telah membandingkan kriptografi kurva eliptik dengan algoritma RSA, untuk panjang kunci kriptografi kurva eliptik yang lebih pendek memiliki tingkat keamanan yang sama dengan RSA. Misalnya, pada kunci kriptografi kurva eliptik sepanjang 160 –bit memberikan keamanan yang sama pada kunci RSA sepanjang 1024 –bit dan kelebihan lain kriptografi kurva eliptik ialah sulitnya memecahkan permasalahan logaritma diskrit kurva eliptik. Akan tetapi, penerapan kurva eliptik dalam kriptografi terkadang digabungkan dengan algoritma kriptografi lainnya seperti menggabungkan kriptografi kurva eliptik dengan kriptosistem kurva eliptik ElGamal untuk meningkatkan keamanan dan efisiensi dalam sistem enkripsi (Munir, 2019).

Kriptosistem kurva eliptik ElGamal adalah varian algoritma ElGamal yang menggunakan prinsip dasar dari kriptografi kurva eliptik untuk meningkatkan

efisiensi dan keamanan (Munir, 2019). Penelitian yang pernah dilakukan oleh Ummu Wachidatul Latifah dan Puguh Wahyu Prasetyo menggunakan kriptosistem kurva eliptik ElGamal yang berjudul "Impelementasi Kriptografi kurva eliptik ElGamal Di Lapangan Galois Prima Pada Proses Enkripsi Dan Dekripsi Berbantuan Perangkat Lunak Python" memberikan kontribusi penting dalam menunjukkan bagaimana algoritma ElGamal dapat diterapkan pada kurva eliptik, baik secara manual maupun dengan bantuan perangkat lunak. Dalam proses pengubahan plainteks menjadi titik pada kurva eliptik, penelitian tersebut menggunakan pendekatan dengan mengalikan nilai desimal dari karakter ASCII langsung dengan titik basis pada kurva. Berbeda dengan pendekatan tersebut, penelitian ini menggunakan metode Koblitz sebagai strategi untuk mengubah plainteks menjadi titik pada kurva eliptik. Metode ini memanfaatkan properti kurva secara lebih sistematis, dengan menjamin bahwa hasil enkoding merupakan titik yang valid pada kurva yang digunakan. Dengan demikian, penelitian ini diharapkan dapat memberikan pendekatan alternatif yang lebih terstruktur dan mendalam dalam proses representasi data teks ke dalam bentuk matematis, sekaligus memperkaya studi implementasi algoritma ElGamal pada kriptografi kurva eliptik.

Berdasarkan permasalahan yang telah diuraikan di atas, dapat dilihat bahwa keamanan data di Indonesia masih menjadi isu yang signifikan dan memerlukan penanganan segera, salah satunya terkait dengan perlindungan data Kartu Tanda Penduduk. Oleh karena itu penelitian mengambil judul penelitian **"IMPLEMENTASI KRIPTOSISTEM KURVA ELIPTIK ELGAMAL UNTUK KEAMANAN DATA PRIBADI PADA KARTU TANDA PENDUDUK"** dengan harapan penelitian ini dapat membantu berbagai pihak dalam mengamankan data.

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah:

1. Bagaimana penerapan kriptosistem kurva eliptik ElGamal berbasis kurva eliptik untuk melakukan enkripsi data pribadi berupa alamat dalam Kartu Tanda Penduduk yang berbentuk teks?
2. Bagaimana menerapkan kriptosistem kurva eliptik ElGamal untuk proses dekripsi cipherteks?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah:

1. Menerapkan dan mendemonstrasikan kriptosistem kurva eliptik ElGamal untuk melakukan enkripsi atau pengamanan data pribadi berupa alamat yang terdapat pada Kartu Tanda Penduduk.

2. Menerapkan dan mendemonstrasikan kriptosistem kurva eliptik ElGamal untuk proses dekripsi cipherteks.

1.4 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah:

1. Data yang digunakan dalam penelitian ini terbatas pada data pribadi berupa alamat yang tercantum pada Kartu Tanda Penduduk, yang dijadikan sebagai bahan simulasi dalam proses enkripsi.
2. Mengenkripsi dan mendekripsi karakter plainteks ASCII yang telah dikodekan menggunakan metode Koblitz.
3. Algoritma kriptografi yang digunakan adalah kriptosistem kurva eliptik ElGamal.

1.5 Manfaat Penelitian

Berdasarkan tujuan dari penelitian, manfaat penelitian adalah:

1. Mampu mengkaji dan menerapkan properti algoritma ElGamal berbasis kurva eliptik dalam proses enkripsi dan dekripsi data pribadi, khususnya alamat pada Kartu Tanda Penduduk.
2. Sebagai bahan referensi dan informasi untuk penelitian selanjutnya.
3. Memberikan informasi dan referensi bagi pembaca mengenai properti algoritma ElGamal pada kurva eliptik serta penerapannya dalam proses enkripsi dan dekripsi plainteks.
4. Menjadi acuan bagi pengembang sistem keamanan digital dalam merancang aplikasi enkripsi data yang efisien, aman, dan sesuai dengan keterbatasan sumber daya sistem (seperti kunci dan memori).