BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi informasi dan pertukaran data dalam era digital telah mengubah fundamental cara berinteraksi dengan dunia sekitar. Dengan peningkatan aksesibilitas internet, *gadget*, dan konektivitas yang semakin meluas, pertukaran informasi telah menjadi lebih cepat, global, dan terintegrasi. Seseorang dapat mengirim pesan instan ke berbagai belahan dunia, berbagi data dalam hitungan detik, dan mengakses pengetahuan dengan mudah melalui platform digital. Bisnis, pendidikan, komunikasi, dan hampir semua aspek kehidupan sehari-hari sangat tergantung pada teknologi informasi. Namun, dengan kemudahan ini juga datang risiko keamanan yang signifikan.

Peningkatan risiko kebocoran data adalah sebuah tantangan yang semakin mendalam seiring dengan pesatnya perkembangan teknologi. Serangan siber, peretasan, dan pelanggaran keamanan menjadi masalah serius yang dapat mengakibatkan kerugian finansial, pencurian identitas, dan bahkan potensi kerugian bagi kepentingan nasional (Suartana dkk., 2022). Selain itu, risiko ini juga mencakup sisi internal, seperti kesalahan manusia dan insiden keamanan yang dapat terjadi di dalam organisasi. Dalam konteks perkembangan teknologi yang pesat, penting untuk menghadapi risiko kebocoran data ini secara serius dan mengambil langkah-langkah proaktif untuk melindungi informasi sensitif.

Dengan demikian, dalam dunia yang semakin terhubung ini, peran kunci keamanan data adalah menjaga agar informasi tetap terpercaya dan bermanfaat bagi individu, organisasi, dan masyarakat secara keseluruhan (Marsaid dkk., 2020). Ada banyak metode yang digunakan untuk mengamankan pesan, contohnya seperti mengamankan pesan dengan menyandikan atau mengubah pesan menjadi pesan tersamar yang tidak bisa terbaca menggunakan suatu algoritma. Ilmu itu disebut *cryptography*.

Kriptografi adalah seni menjaga keamanan informasi dengan mengubah suatu informasi yang dapat dipahami menjadi suatu bentuk yang tidak dapat dipahami oleh penerima yang tidak diinginkan. Pesan asli yang dapat dibaca

manusia disebut sebagai plainteks (*plaintext*), kemudian pesan ini diproses menggunakan algoritma tertentu menjadi pesan tersamar (*ciphertext*) yang tidak dapat dipahami maknanya. Algoritma kriptografi dapat digunakan untuk mentransfer informasi secara aman antara dua pihak tanpa diintervensi oleh elemen eksternal (Noviyanti & Mira, 2022).

Penggunaan kriptografi sangat penting dalam melindungi data sensitif di era digital. Dengan kriptografi, data diubah menjadi format yang hanya dapat didekripsi dengan kunci yang benar. Artinya, meskipun data jatuh ke tangan yang salah, data tersebut tetap tidak dapat dibaca atau dipahami. Bagi individu, ini berarti melindungi informasi pribadi seperti kata sandi, data keuangan, atau catatan medis. Pada tingkat organisasi, kriptografi memberikan landasan penting untuk menjaga keamanan data bisnis, desain produk, atau strategi perusahaan.

Bahkan di tingkat keamanan pemerintah dan nasional, kriptografi masih digunakan untuk melindungi komunikasi dan data penting. Sebagai contoh, negara-negara sering menggunakan kriptografi untuk mengamankan komunikasi antar lembaga pemerintahan, militer, dan agensi intelijen. Penggunaan kriptografi ini membantu mencegah pihak yang tidak berwenang dari memata-matai atau mengganggu komunikasi yang bersifat strategis. Selain itu, di tingkat pemerintahan, kriptografi digunakan untuk melindungi data sensitif, seperti informasi keuangan, data warga negara, dan dokumen hukum, yang harus tetap aman dan tidak tersentuh oleh pihak yang tidak berhak. Dengan demikian, kriptografi memainkan peran krusial dalam menjaga integritas dan keamanan negara (Gajcowski & Jenkins, 2022).

Oleh karena itu, pentingnya penggunaan kriptografi adalah untuk melindungi data sensitif dari risiko kebocoran dan peretasan, melindungi privasi individu, serta menjamin kelangsungan bisnis dan keamanan nasional di masa depan. Beberapa algoritma kriptografi yang tersedia antara lain *Caesar Cipher*, *Vigenere Cipher*, *Hill Cipher*, *RSA*, *Advanced Encryption Standard* (AES), *Elliptic Curve Cryptography* (ECC), dan lainnya.

Kriptografi terbagi menjadi dua, yaitu kriptografi klasik/simetris dan kriptografi kunci publik/asimetris. Kriptografi klasik menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi pesan (Pratiwi & Asmunin, 2022). Ini

berarti bahwa pihak yang terlibat dalam komunikasi perlu berbagi kunci enkripsi yang rahasia, yang memungkinkan mereka untuk berkomunikasi secara aman. Keuntungan utama dari kriptografi simetris adalah kecepatan dan efisiensi dalam pengolahan data, membuatnya ideal untuk enkripsi data dalam jumlah besar. Algoritma kriptografi simetris yang umum digunakan antara lain *Caesar Cipher, Vigenere Cipher, Hill Cipher, dan Advanced Encryption Standard* (AES) (Pratiwi & Asmunin, 2022).

Di sisi lain, kriptografi asimetris menggunakan sepasang kunci yang berbeda: kunci publik yang digunakan untuk enkripsi pesan dan kunci pribadi yang hanya dimiliki oleh penerima pesan untuk mendekripsinya (Listiani dkk., 2022). Ini membuatnya lebih aman dalam hal pertukaran kunci, karena tidak perlu berbagi kunci pribadi. Namun, kriptografi asimetris cenderung lebih lambat dalam pemrosesan data dibandingkan dengan simetris. Oleh karena itu, penggunaan kriptografi simetris dan asimetris sering digabungkan dalam pendekatan kriptografi *hybrid*, yang memadukan keuntungan dari keduanya: kecepatan dari simetris dan keamanan pertukaran kunci dari asimetris.

Penggabungan kriptografi *hybrid* dapat meningkatkan keamanan komunikasi digital dengan memadukan kelebihan dari kriptografi simetris dan asimetris (Putra dkk., 2023). Dalam pendekatan ini, kriptografi simetris digunakan untuk mengenkripsi pesan dengan kunci bersama yang relatif lebih cepat dan efisien dalam hal kinerja. Sementara itu, kriptografi asimetris digunakan untuk mengenkripsi kunci simetris yang digunakan dalam enkripsi pesan, dan juga untuk proses autentikasi (Yonathan dkk., 2021).

Kelebihan utama dari pendekatan ini adalah bahwa, meskipun kunci simetris perlu disampaikan melalui saluran yang aman, kunci asimetris yang jauh lebih panjang dan kompleks digunakan untuk mengamankan pertukaran kunci ini. Ini mengatasi salah satu tantangan utama kriptografi simetris, yaitu masalah distribusi kunci yang aman (Hamidah, 2009). Dengan demikian, penggabungan kriptografi *hybrid* memungkinkan efisiensi komputasi dengan keamanan yang tinggi, yang menjadikannya pendekatan yang sangat efektif dalam melindungi komunikasi digital yang sensitif Dalam hal ini, algoritma kriptografi yang dipilih adalah algoritma AES (simetris) dan algoritma ECC (asimetris).

Advanced Encryption Standard (AES) adalah sebuah algoritma kriptografi yang digunakan untuk mengamankan data dalam komunikasi elektronik. AES menggunakan teknik pengamanan dengan mengenkripsi data menggunakan blok-blok data yang berukuran 128 bit, 192 bit, atau 256 bit (Rothke, 2011). Keuntungan dari AES adalah memiliki keamanan yang tinggi dan efisiensi yang baik karena proses enkripsi dan dekripsinya lebih cepat dibanding dengan algoritma RSA. hal ini dikarenakan panjang kunci yang digunakan pada AES hanyalah 128, 192, atau 256-bit sedangkan RSA menggunakan kunci sepanjang 2048 atau 3072 bit. (Rothke, 2011). Kecepatan dari algoritma AES adalah kurang lebih 236x lebih cepat saat proses enkripsi dibandingkan dengan algoritma RSA (Anwar dkk., 2018).

Elliptic Curve Cryptography (ECC) adalah sebuah teknik kriptografi yang menggunakan kurva eliptik dalam operasinya yang digunakan untuk mengamankan data dalam komunikasi elektronik, seperti email, pesan teks, dan transaksi finansial online. Keuntungan dari ECC adalah ukuran kunci yang lebih kecil dibandingkan dengan algoritma kriptografi lainnya seperti RSA, sehingga lebih efisien dalam penggunaannya. Selain itu, ECC juga lebih aman karena sulit untuk dipecahkan oleh serangan *brute force* dan serangan lainnya dikarenakan banyak sekali kemungkinan untuk menemukan kunci yang tepat. Dibutuhkan waktu yang sangat lama untuk meretas algoritma ini menggunakan perangkat komputer (Abdelfatah, 2020).

Selain dengan menyandikan pesan, ada juga metode pengamanan pesan dengan cara menyembunyikan pesan ke dalam media lain seperti gambar, video, audio, maupun media lainnya agar orang lain tidak dapat melihat pesan yang disembunyikan di dalam media. Ilmu ini disebut steganografi. Steganografi adalah seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia (Munir, 2019). Salah satu metode steganografi dalam pengamanan pesan adalah *Least Significant Bit*.

Least Significant Bit (LSB) adalah teknik yang digunakan dalam steganografi untuk menyembunyikan data rahasia dalam media digital seperti gambar, suara, dan video. Teknik ini bekerja dengan mengubah bit terakhir dari media yang digunakan untuk menyimpan data rahasia. Teknik LSB merupakan

salah satu teknik yang paling umum digunakan dalam steganografi karena sederhana dan efektif (Lutfi & Rosihan, 2018)

Penelitian mengenai kriptografi *hybrid* AES dan ECC telah dilakukan oleh Sibarani dkk. (2017). Mereka menyimpulkan bahwa penggabungan metode AES dan ECC dapat meningkatkan keamanan suatu data dan mempercepat proses pengamanan data. Penelitian tersebut hanya menggunakan algoritma kriptografi *hybrid* AES dan ECC, namun belum menggunakan metode steganografi sebagai teknik penyembunyian hasil enkripsi ke dalam gambar. Penelitian mengenai penggabungan kriptografi *hybrid* dengan steganografi juga telah dilakukan oleh (Dewi dkk., 2022). Mereka menyimpulkan penggabungan metode ini bisa menyembunyikan keberadaan pesan dari pelaku yang ingin melakukan penyadapan. Selain itu, hasil dari proses *embedding* tidak menunjukkan perubahan warna yang signifikan bahkan terkesan tidak memiliki perubahan sama sekali.

Penelitian ini berfokus pada pengembangan dari peningkatan keamanan dengan menggunakan algoritma kriptografi *hybrid* AES dan ECC yang digabungkan dengan steganografi LSB dalam mengamankan pesan dengan cara mengenkripsi pesan memakai metode *hybrid* AES dan ECC lalu menyembunyikan hasil enkripsi ke dalam objek gambar dengan metode LSB. Pemilihan objek gambar bertujuan untuk menyembunyikan pesan rahasia dan mengurangi kecurigaan dari pihak-pihak yang tidak berkepentingan dalam mengambil informasi pesan rahasia tersebut. Metode dalam penelitian ini diharapkan mampu untuk menjaga kerahasiaan dan menyembunyikan pesan dari pihak yang tidak berkepentingan dengan cara menggabungkan teknik kriptografi *hybrid* dan steganografi. Untuk mempermudah proses dalam pembangkitan kunci, enkripsi, dekripsi, dan penyisipan pesan dalam gambar maka akan dibuat program aplikasi komputernya menggunakan *Python.*

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang, maka permasalahan yang dirumuskan adalah sebagai berikut:

1. Bagaimana cara mengamankan pesan menggunakan kriptografi *hybrid* AES dan ECC dengan steganografi LSB ke dalam gambar?

2. Bagaimana implementasi kriptografi *hybrid* AES dan ECC dengan steganografi LSB dalam bentuk program aplikasi menggunakan bahasa pemrograman *Python*?

1.3 Tujuan Penelitian

Tujuan penelitian yang dapat ditetapkan berdasarkan rumusan masalah adalah:

1. Untuk mengetahui cara mengamankan pesan menggunakan penggabungan kriptografi *hybrid* AES dan ECC dengan steganografi LSB ke dalam gambar.
2. Untuk mengimplementasikan metode kriptografi *hybrid* AES dan ECC dengan steganografi LSB dalam bentuk program aplikasi menggunakan bahasa pemrograman python.

1.4 Manfaat Penelitian

1. Manfaat Teoretis

   Penelitian ini diharapkan dapat berkontribusi terhadap pengembangan dalam bidang matematika terapan melalui pengembangan kriptografi khususnya dalam algoritma AES dan ECC.

2. Manfaat Praktis

   Dapat menjaga kerahasiaan dan keaslian pesan yang telah dienkripsi serta menyamarkan keberadaan pesan dengan menyisipkan pesan ke dalam gambar, sehingga kerahasiaannya akan terjaga.

1.5 Batasan Masalah Penelitian

1. Pesan yang digunakan berupa data teks yang karakter-karakternya termasuk dalam rentang ASCII 32 hingga 126.
2. Jenis kriptografi AES yang digunakan adalah AES-128.
3. Ukuran data teks harus lebih kecil dari ukuran data gambar.