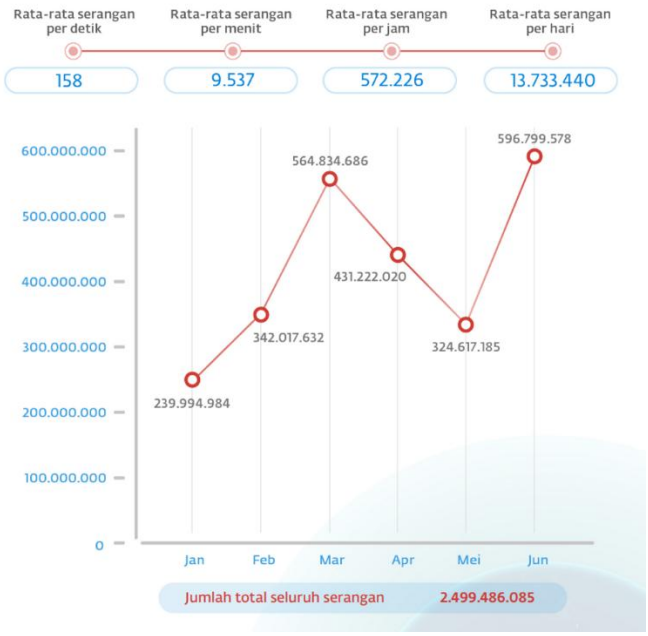
BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Penggunaan internet dan teknologi telah menjadi peran besar dalam kehidupan sehari-hari masyarakat modern. Melimpahnya informasi di era teknologi saat ini menuntut untuk memberi perhatian yang lebih besar terhadap aspek keamanan. Namun, tantangan terkait keamanan data dan privasi yang semakin kompleks di dunia digital menuntut masyarakat untuk meningkatkan kesadaran dan perlindungan terhadap risiko tersebut. Menjaga keamanan dan kerahasiaan data diperlukan terutama dalam proses berbagi informasi antara beberapa pihak. Upaya ini penting dilakukan untuk melindungi informasi dari akses yang tidak berwenang, menjaga keutuhan data, serta memastikan keamanan operasional sistem komputer secara menyeluruh (Manurung dkk., 2023). Seperti yang terlihat pada Gambar 1.1, pada grafik laporan jumlah serangan *cyber* di Indonesia cenderung meningkat selama semester 1 tahun 2024.



Gambar 1.1 Jumlah serangan *cyber* di Indonesia selama semester 1 2024 (AwanPintar.id, 2024)

Raoul Khakim Annur, 2025
IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES DAN NOISELESS STEGANOGRAFI AUDIO UNTUK PENGAMANAN DATA TEKS BERBASIS APLIKASI WEB
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Berdasarkan Gambar 1.1, dapat disimpulkan bahwa banyak serangan siber yang terjadi di Indonesia dalam kurun waktu yang singkat. Menunjukkan dengan jelas bahwa serangan siber berskala nasional memerlukan perhatian serius. Lonjakan ancaman yang meningkat berkali-kali lipat menjadi indikasi adanya berbagai celah dalam sistem keamanan nasional. Oleh karena itu, diperlukan kepedulian kolektif, terutama dari para profesional di bidang IT, untuk segera mengambil langkah-langkah inovatif, progresif, dan preventif guna melindungi kepentingan bangsa serta mewujudkan kedaulatan siber negara (AwanPintar.id, 2024).

Menurut laporan Badan Siber dan Sandi Negara (BSSN) tahun 2024, sebanyak 241 insiden kebocoran data terdeteksi selama tahun 2024, dengan sektor pemerintahan menjadi yang paling terdampak. Laporan yang sama juga mengungkapkan bahwa lebih dari 56 juta data terekspos di *darknet*, menunjukkan meningkatnya ancaman terhadap integritas dan kerahasiaan informasi digital di Indonesia. Kondisi ini menandakan bahwa perlindungan terhadap data teks, khususnya yang bersifat sensitif seperti informasi pribadi atau kredensial, menjadi semakin penting. Ancaman seperti *phishing*, *malware*, hingga eksploitasi celah keamanan memperburuk risiko kebocoran data yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab (BSSN, 2024).

Berbagai insiden seperti pencurian data pribadi, peretasan akses, dan penyalahgunaan informasi telah menjadi ancaman nyata di dunia digital. Data teks, sebagai salah satu bentuk informasi yang paling umum digunakan dalam komunikasi digital, rentan terhadap serangan seperti penyadapan dan manipulasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, diperlukan langkah-langkah untuk melindungi data teks (Khairani & Siambaton, 2023).

Salah satu pendekatan yang dapat digunakan untuk meningkatkan keamanan data adalah dengan menggabungkan metode kriptografi dan steganografi. Kriptografi bertujuan untuk mengenkripsi data agar tidak dapat diakses oleh pihak yang tidak memiliki kunci, sedangkan steganografi menyembunyikan keberadaan data dengan cara menyisipkannya ke dalam media lain, seperti gambar, audio, atau video. Kombinasi kedua metode ini memberikan lapisan keamanan ganda yang sulit untuk

ditembus, karena data tidak hanya terenkripsi tetapi juga tidak terdeteksi keberadaannya (Prasetiyo dkk., 2015).

Metode kriptografi *Advanced Encryption Standard* (AES) merupakan salah satu algoritma enkripsi yang banyak digunakan karena tingkat keamanannya yang tinggi dan efisiensi prosesnya. Enkripsi data merupakan metode utama untuk melindungi keamanan dan kerahasiaan informasi yang ditransmisikan melalui jaringan komputer. Proses enkripsi bekerja dengan mengubah data teks asli (*plaintext*) yang mudah dipahami menjadi bentuk terenkripsi (*ciphertext*) yang tidak terbaca oleh manusia. Hanya pihak yang memiliki kunci dekripsi yang sesuai yang mampu mengembalikan data terenkripsi tersebut ke bentuk aslinya, sehingga memastikan bahwa informasi sensitif tetap aman dari akses tidak sah selama proses pertukaran (Wachid Hidayatulloh dkk., 2023). Keunggulan algoritma AES memiliki fleksibilitas dengan ukuran kunci yang bervariasi, seperti 128-bit dan 256-bit, yang memberikan perlindungan lebih terhadap upaya serangan (Andriyanto & Sukmasetya, 2022).

Hasil dari proses enkripsi (*ciphertext*) berupa teks acak yang tidak dapat dipahami atau diterjemahkan tanpa melalui proses dekripsi. Namun, hal ini dapat memicu kecurigaan pihak lain yang mungkin berniat menyalahgunakan atau merusak pesan rahasia tersebut. Oleh karena itu, *ciphertext* akan disisipkan ke dalam citra dengan menggunakan teknik *steganografi*. Dalam penerapannya, *steganografi* berfungsi untuk menyembunyikan pesan rahasia di dalam suatu informasi tanpa menimbulkan kecurigaan, sehingga keberadaannya tetap tersembunyi selama proses pengiriman (Umam & Muslih, 2023). Secara umum, teknik yang digunakan adalah mengenkripsi pesan terlebih dahulu menggunakan algoritma kriptografi dan menghasilkan *ciphertext*, lalu menyembunyikan pesan terenkripsi tersebut ke dalam media lain (suara, teks, video, atau gambar) melalui metode steganografi. Namun, pada steganografi konvensional, penyembunyian pesan dapat mengurangi kualitas media penampung (*cover*), metode *Noiseless Steganography* atau NoStega justru tidak menimbulkan kerusakan atau *noise* pada media tersebut (Juhari & Andrean, 2022).

Oleh sebab itu, *ciphertext* disembunyikan dengan cara diubah menjadi *file* audio dengan memanfaatkan teknik *Noiseless Steganography*. Konsep NoStega (*Noiseless*

Steganography) tidak menyembunyikan data dalam *noise* ataupun mengubahnya menjadi bentuk *noise*. Sebaliknya, NoStega menyamarkan pesan dalam bentuk data yang tidak dapat menimbulkan kecurigaan dalam *cover* yang dihasilkan dari pesan tersebut (Desoky, 2012).

Dalam penelitian ini, metode kombinasi AES dan NoStega diterapkan untuk pengamanan data teks berbasis aplikasi web. Aplikasi ini dirancang untuk mengenkripsi data teks menggunakan algoritma AES, lalu merubah data terenkripsi tersebut menjadi *file* audio menggunakan teknik *noiseless steganografi*. Dengan pendekatan ini, diharapkan data teks dapat dilindungi secara efektif dari akses yang tidak sah, serta memberikan solusi praktis bagi pengguna dalam menjaga privasi dan keamanan informasi digital.

1.2. Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah dijelaskan, maka didapat beberapa rumusan masalah penelitian sebagai berikut:

1. Bagaimana merancang aplikasi web yang dapat menerapkan teknik *noiseless steganography* dan kriptografi AES?
2. Bagaimana cara mengimplementasikan algoritma kriptografi AES untuk enkripsi teks dan mengubah hasil enkripsi tersebut menjadi *file* audio?
3. Bagaimana efektivitas teknik *noiseless steganography* dalam menyembunyikan informasi rahasia tanpa menimbulkan kecurigaan ?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah penelitian, maka didapat tujuan dari penelitian sebagai berikut:

1. Merancang aplikasi berbasis web yang menerapkan teknik *noiseless steganography* dan kriptografi AES.
2. Mengimplementasikan algoritma kriptografi AES untuk enkripsi teks dan mengubahnya menjadi *file* audio.
3. Dapat menilai dan mengevaluasi sejauh mana teknik *noiseless steganography* dapat menyembunyikan informasi rahasia tanpa menimbulkan kecurigaan terhadap data yang terenkripsi.

1.4. Manfaat Penelitian

Merujuk pada tujuan yang telah diuraikan sebelumnya, penelitian ini diharapkan mampu memberikan kontribusi dalam pengembangan teknologi, khususnya di ranah *cybersecurity* dan keamanan data. Beberapa manfaat yang diharapkan bisa didapat dari penelitian ini dijabarkan sebagai berikut:

1.4.1. Manfaat Teoritis

1. Diharapkan penelitian ini dapat menjadi acuan baru bagi studi selanjutnya dengan topik serupa, sehingga penelitian yang dihasilkan dapat dikembangkan lebih mendalam.
2. Penelitian ini dapat menambah pengetahuan pada bidang keamanan data, khususnya pada algoritma kriptografi AES dan teknik *Noiseless Steganography* (NoStega).
3. Diharapkan penelitian ini bisa menjadi landasan inovasi baru dalam metode mengamankan data teks dengan NoStega

1.4.2. Manfaat Praktis

1. Penelitian ini memberikan alternatif untuk mengamankan data teks dari akses yang tidak berkepentingan dengan enkripsi AES yang setelahnya diproses dengan teknik NoStega.
2. Aplikasi yang dikembangkan berbasis website pada penelitian ini digunakan untuk meningkatkan keamanan data teks pengguna, dibungkus dengan tampilan antarmuka yang *user-friendly* sehingga dapat digunakan dengan mudah tanpa memerlukan keahlian teknis tertentu.
3. Hasil implementasi dari penelitian ini diharapkan dapat memberikan kontribusi dalam mendukung kebutuhan pertukaran informasi rahasia antar pengguna yang memprioritaskan keamanan data teks. Dengan sistem perlindungan yang dirancang, penelitian ini mampu memastikan kerahasiaan data teks selama proses pertukaran informasi, sehingga meminimalkan risiko akses oleh pihak yang tidak berwenang.

1.5. Ruang Lingkup Penelitian

Agar penelitian ini dapat dikerjakan dengan maksimal dan membatasi cakupan penelitian, maka diperlukan batasan-batasan sebagai berikut:

1. Media yang dienkripsi difokuskan pada data teks.
2. Penelitian ini menggunakan algoritma *Advanced Encryption Standard* (AES) untuk enkripsi teks dan teknik NoStega untuk mengubah *ciphertext* menjadi *file* audio.
3. Proses *generate* audio dalam penelitian ini hanya menggunakan satu jenis lagu, yaitu "Mary Had A Little Lamb".
4. Format file audio yang digunakan dalam penelitian ini dibatasi hanya pada format WAV.
5. Penelitian ini tidak menyediakan fitur untuk mengunggah *file* audio sebagai input enkripsi, hanya mengakomodir input *plaintext* sebagai pesan rahasia.
6. Kapasitas input *plaintext* dibatasi hingga 5.386 karakter, karena *library* SciPy hanya mengakomodir format WAV 32-bit.
7. Proses dekripsi hanya dapat dilakukan pada file audio yang merupakan hasil dari proses enkripsi dan steganografi dari aplikasi ini. Hal ini memastikan integritas dan keamanan pesan yang telah disisipkan.