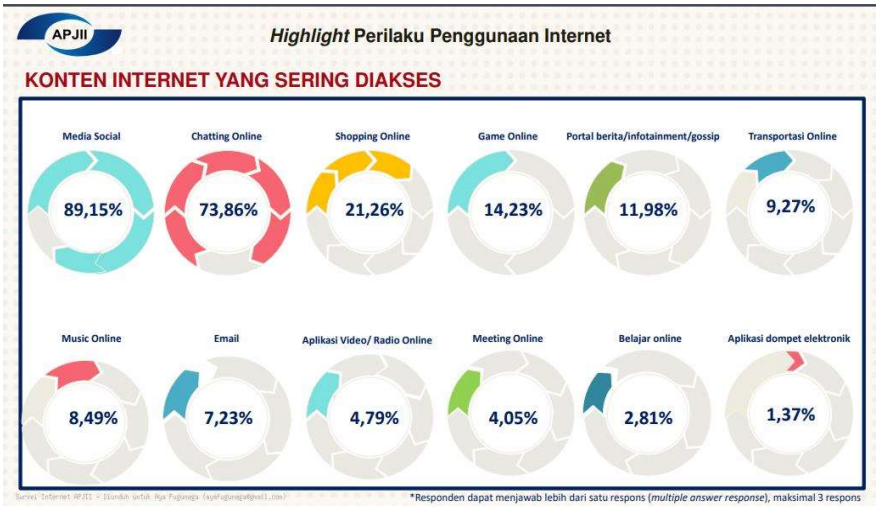
BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi yang pesat khususnya di bidang komputasi memerlukan perbaikan sistem keamanan secara terus menerus untuk melindungi data dan dokumen dari potensi ancaman keamanan. Hal ini penting untuk menjaga kerahasiaan informasi dari akses yang tidak sah, memastikan integritas data, dan melindungi keamanan operasional sistem komputer secara keseluruhan (Handoyo & Subakti, 2020). Oleh karena itu, pengembangan keamanan data diperlukan untuk melindungi data rahasia yang dikirimkan melalui jaringan komunikasi.

Dengan banyaknya penggunaan internet pada masa kini, keamanan data menjadi hal yang dibutuhkan dalam pengiriman data berupa *file* maupun bentuk lainnya. Banyak sekali kejadian yang merugikan jika data tersebut didapatkan oleh pihak yang tidak bertanggung jawab, Seperti penggunaan data pribadi untuk menipu, mencuri, atau hal lainnya yang berpotensi terjadinya kerugian dalam jumlah yang besar.



Gambar 1.1 Konten Internet yang Sering Diakses (Arif, 2022)

Berdasarkan Gambar 1.1, dapat disimpulkan bahwa banyak pengguna internet menggunakan layanan *online* untuk keperluan seperti media sosial, *chatting online*, dan belanja *online*. Jika dihubungkan dengan pembahasan sebelumnya tentang adanya peretasan terhadap data sensitif dari penggunaan internet, menjadi penting untuk menjaga kerahasiaan dan meningkatkan kesadaran terhadap data sensitif saat berselancar di internet. Beberapa jenis pengamanan data sensitif yang ada antara

lain DES, RC5, dan AES. Dari ketiga jenis keamanan ini memiliki kelebihan dan kekurangannya masing-masing yaitu keamanan DES yang sudah terlalu usang dan lambat, RC5 menjadi pilihan yang baik akan tetapi keamanan ini telah dipatenkan. adapun AES yang menjadi pilihan terbaik dan banyak digunakan juga penerapannya pada program keamanan (Rinaldi Munir, 2020). Oleh Karena itu Penulis pada penelitian ini menggunakan AES sebagai algoritma keamanan.

Algoritma AES banyak digunakan untuk mengamankan data pengguna aktif di internet dan melindungi komunikasi bisnis yang sensitif. Keunggulan AES dalam melindungi data sensitif melalui kunci enkripsi yang kuat menjadikannya pilihan utama di berbagai bidang, termasuk keuangan, kedokteran, militer, dan komunikasi. AES secara efektif melindungi informasi sensitif dan transaksi sensitif yang sulit diretas dengan teknologi *brute force* saat ini. AES menghasilkan enkripsi yang kuat, apalagi dengan adanya steganografi untuk memperkuat hasil dari AES. Steganografi adalah ilmu dan bisa dikatakan seni menyembunyikan pesan rahasia dengan suatu cara sedemikian rupa sehingga sedikit orang yang mencurigai keberadaan pesan yang telah disembunyikan. Steganografi ini bisa berbentuk audio, video, teks, dan gambar (Sagar Hossen dkk., 2020). Teknik ini memudahkan untuk menyembunyikan informasi rahasia dalam hasil enkripsi AES untuk memperkuat keamanan (Kurnia Nurhareza & Siswanto, 2022). *Graphstega* adalah metode steganografi yang menyematkan pesan sebagai data yang diplot ke dalam sebuah grafik. *Graphstega* dapat menyamarkan pesan. *Graphstega* tahan terhadap serangan modern, seperti analisis lalu lintas dan serangan perbandingan(Ashari & Munir, 2018). Kelemahan yang ada pada penelitian sebelumnya adalah *ciphertext* dari hasil enkripsi yang terlihat dan peretas dapat menaruh kecurigaan terhadap *file* tersebut (Widodo & Purnomo, 2020). Penelitian ini menggunakan steganografi untuk menyembunyikan data sensitif dalam hasil enkripsi AES. Dengan menggunakan keamanan AES sebagai landasan, penelitian ini membuka peluang pengembangan teknik steganografi yang lebih maju dan efektif yang mengintegrasikan keamanan dan kerahasiaan di era digital yang terus berkembang (Sagar Hossen dkk., 2020).

Urgensi penelitian ini adalah untuk mengurangi kecurigaan pihak-pihak yang tidak bertanggung jawab terhadap hasil enkripsi AES yang disisipi pada diagram

garis menggunakan teknik steganografi dengan metode *graphstega* sehingga upaya dekripsi hasil enkripsi yang terlihat dapat dikurangi ataupun dihilangkan. Peneliti memilih teknik steganografi dengan metode *graphstega* dan kriptografi AES ini menggunakan visualisasi diagram garis dengan tema saham (Ida Hendarsih, 2016). Dikarenakan visualisasi grafik saham salah satunya dengan menggunakan Diagram garis, maka tema saham lah yang diambil sebagai *cover* dalam teknik steganografi dengan metode *graphstega* yang peneliti gunakan. Dengan mengembangkan teknik steganografi yang dapat menyembunyikan informasi sensitif dalam hasil enkripsi AES, diharapkan dapat melindungi data sensitif dari pihak yang tidak berwenang. Penerapan teknologi ini peneliti berharap dapat meminimalisir kecurigaan terhadap *file* hasil enkripsi yang berbentuk diagram garis dan juga dengan menggunakan enkripsi AES sebagai algoritma enkripsi dapat memperkuat hasil *ciphertext* dari aplikasi yang dikembangakan oleh peneliti. Penelitian ini akan menerapkan teknik steganografi dengan metode *graphstega* dan kriptografi AES berbasis aplikasi web yang dapat diakses secara umum dengan menggunakan akses internet dan teknologi yang mendukung.

1.2 Rumusan Masalah Penelitian

Berdasarkan konteks yang telah diuraikan sebelumnya, peneliti merumuskan beberapa pertanyaan penelitian, yaitu:

1. Bagaimana merancang aplikasi web yang dapat menerapkan teknik steganografi dengan metode *Graphstega* dan kriptografi AES?
2. Apakah enkripsi AES menyediakan keamanan yang memadai?
3. Apakah metode *Graphstega* dalam steganografi dapat mengurangi kecurigaan visual terhadap data yang terenkripsi?

1.3 Batasan Penelitian

Batasan penelitian diperlukan untuk memandu fokus penelitian dan menghindari risiko perluasan cakupan penelitian secara berlebihan. Keterbatasan penelitian ini meliputi:

1. Penelitian ini hanya mempelajari teknik steganografi yang diterapkan pada hasil enkripsi AES.
2. Fokus penelitian adalah menyembunyikan data hasil enkripsi AES tanpa mengurangi kekuatan keamanan dari enkripsi itu sendiri.

3. Penelitian ini tidak mencakup analisis perbandingan dengan algoritma enkripsi lain selain AES.
4. Implementasi steganografi diuji dalam lingkungan simulasi, bukan pada skala produksi.
5. Penelitian ini menggunakan data uji standar dan menyertakan data nyata hasil enkripsi apakah mencurigakan atau tidak dari pengguna untuk mengetahui kesamaran data hasil enkripsi.
6. Penelitian ini berfokus untuk mengetahui apakah *cover* yang dihasilkan oleh enkripsi dapat tersamarkan dengan baik.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan sebelumnya, tujuan dari penelitian ini adalah:

1. Merancang aplikasi web yang dapat menerapkan teknik steganografi dengan metode *Graphstega* dan kriptografi AES
2. Menilai bagaimana teknologi enkripsi AES dapat menyediakan keamanan yang memadai
3. Mengetahui sejauh mana metode *Graphstega* dalam steganografi dapat mengurangi kecurigaan visual terhadap data yang terenkripsi

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian di atas, maka penelitian ini diharapkan dapat memberikan kontribusi khususnya dalam hal keamanan informasi perusahaan. Beberapa manfaat yang diharapkan dari penelitian ini antara lain:

1.5.1 Manfaat Teoritis

1. Penelitian ini dapat memperluas wawasan dan pengetahuan di bidang kriptografi khususnya dalam konteks pengembangan AES sebagai Algoritma keamanan data.
2. Hasil penelitian ini dapat menjadi referensi bagi penelitian selanjutnya yang bertujuan untuk mengembangkan teknik steganografi dalam konteks enkripsi data.

1.5.2 Manfaat Praktis

1. Penelitian ini memberikan solusi praktis untuk melindungi data sensitif dari akses tidak sah dengan menggunakan enkripsi AES yang dikombinasikan dengan teknik steganografi.
2. Dengan menerapkan teknik ini, perusahaan dapat meningkatkan keamanan komunikasi data dan mengurangi risiko tersebarnya informasi penting.
3. Memberikan solusi bagi para profesional keamanan informasi untuk menerapkan teknologi enkripsi yang lebih aman dan efektif dalam lingkungan bisnis sehari-hari.

Oleh karena itu, penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam dan lebih baik mengenai penggunaan algoritma AES untuk meningkatkan keamanan informasi di perusahaan.

1.6 Struktur Organisasi Skripsi

Sistem penulisan karya ilmiah terdiri dari lima bagian utama: pendahuluan, tinjauan pustaka, metode penelitian, hasil dan pembahasan, serta kesimpulan, implikasi, dan rekomendasi. Hal ini berdasarkan Peraturan Rektor UPI (Universitas Pendidikan Indonesia) Nomor 7867/UN40/HK/2021 tentang Pedoman Penulisan Naskah Akademik Universitas Pendidikan Indonesia Tahun 2021. Detail masing-masing bagian adalah sebagai berikut:

1. PENDAHULUAN

   Bagian ini menguraikan latar belakang masalah, rumusan masalah, tujuan penelitian, kelebihan penelitian, dan keterbatasan penelitian. Pendahuluan memberikan gambaran tentang topik yang sedang dipelajari dan mengapa penelitian itu penting. bagian ini pun yang menjadi alasan penulisan.

2. KAJIAN PUSTAKA

   Bagian kedua ini disebut Kajian Pustaka. Kajian Pustaka menyoroti Kajian teoritis dari penelitian sebelumnya tentang topik penelitian yang serupa. Fokus bab ini adalah memahami metode AES dan membuat grafik garis dalam konteks penelitian steganografi. Bagian ini mengulas literatur tentang prinsip dasar enkripsi, cara kerja AES, dan teknik steganografi untuk menyembunyikan data dalam hasil terenkripsi AES. Disini penulis

memberikan beberapa ringkasan literatur yang mendukung penelitian dan menjadi dasar penelitian yang dilakukan.

3. METODE PENELITIAN

Bagian ketiga, yaitu Metodologi Penelitian, merinci langkah-langkah yang diambil dalam proses penelitian, dimulai dari perancangan, implementasi, hingga pengujian model enkripsi AES.

4. TEMUAN DAN PEMBAHASAN

Di bagian Hasil dan Pembahasan, Peneliti menguji hasil enkripsi AES yang diubah menjadi grafik garis menggunakan teknik steganografi dan mengevaluasi hasil pengujiannya. Bagian ini juga menjelaskan Kelebihan dan kekurangan sistem yang diusulkan.

5. SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Bagian yang berjudul Simpulan, Implikasi, dan Rekomendasi ini merupakan gambaran umum dari seluruh penelitian yang dilakukan. Kesimpulan memuat hasil utama penelitian yang menyoroti pencapaian tujuan penelitian dan jawaban atas rumusan pertanyaan yang diajukan. Implikasi penelitian ini dibahas untuk menempatkan hasilnya dalam konteks yang lebih luas, baik secara teori maupun praktik. Selain itu, rekomendasi diberikan untuk memandu langkah lebih lanjut yang dapat diambil untuk meningkatkan atau memperluas penelitian ini di masa depan.