# BAB I

# PENDAHULUAN

## 1.1. Latar Belakang

Dalam era digital yang semakin berkembang, keamanan informasi menjadi salah satu aspek yang sangat penting, terutama dalam konteks komunikasi resmi di instansi pemerintah Sebagai lembaga yang bertanggung jawab atas pengelolaan informasi publik, Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo, penggunaan email sebagai sarana komunikasi sehari-hari membawa tantangan tersendiri terkait perlindungan data. Informasi yang dikirimkan melalui email sering kali mengandung data sensitif yang jika jatuh ke tangan yang salah dapat menimbulkan dampak negatif, baik bagi instansi maupun masyarakat. Oleh karena itu, menggunakan metode kriptografi adalah langkah penting untuk menjaga kerahasiaan dan integritas data yang dikirimkan.

Kriptografi merupakan bidang yang sangat penting dalam menjaga keamanan informasi Di era digital saat ini, perlindungan informasi menjadi semakin penting. Seiring dengan pesatnya perkembangan teknologi informasi dan komunikasi, ancaman terhadap data sensitif juga turut meningkat, baik akibat serangan siber maupun kebocoran data. Untuk mengatasi hal ini, kriptografi memainkan peran vital dalam menjaga kerahasiaan, integritas, dan keaslian informasi dengan cara mengenkripsi dan mendekripsi data. Proses enkripsi mengubah data asli (plaintext) menjadi bentuk terenkripsi (ciphertext) yang tidak dapat dibaca tanpa kunci yang sesuai. Dengan demikian, hanya pihak yang berwenang yang dapat mengakses informasi tersebut. Perlindungan semacam ini sangat penting terutama dalam komunikasi resmi, transaksi finansial, dan penyimpanan data yang bersifat rahasia.(Maulana Iqbal, 2024)

(El Anwar et al., 2022) kriptografi menggunakan metode Advanced Encryption Standard (AES) terbukti sangat efektif dalam melindungi data dari akses tidak sah. AES, yang merupakan algoritma enkripsi simetris, mampu mengenkripsi data dengan ukuran blok 128 bit dan mendukung kunci dengan panjang 128, 192, dan 256 bit.

(Rachma Putra & Sidqon, 2024) Advanced Encryption Standard (AES) 256 bit adalah algoritma enkripsi simetris yang dirancang untuk memberikan tingkat keamanan tinggi dalam pengolahan data. Dengan panjang kunci 256-bit, AES mampu melindungi informasi sensitif dari berbagai ancaman, termasuk serangan yang mencoba menebak kunci secara berulang. Algoritma ini telah diadopsi secara luas dalam berbagai aplikasi, mulai dari komunikasi pemerintah hingga transaksi keuangan, berkat kemampuannya dalam menjaga kerahasiaan dan integritas data. Dengan demikian, AES 256-bit menjadi pilihan utama untuk memastikan keamanan informasi di era digital saat ini.

## 1.2. Rumusan Masalah

Berdasarkan pada latar belakang, Maka rumusan masalah pada penelitian ini adalah :

1. Bagaimana penerapan metode kriptografi, khususnya algoritma Advanced Encryption Standard (AES), dapat meningkatkan kerahasiaan dan integritas informasi dalam email di Dinas Komunikasi dan Informatika Provinsi Gorontalo?
2. Apa tantangan utama yang dihadapi oleh Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo dalam menerapkan Tanda Tangan Elektronik (TTE) untuk memastikan keamanan data sensitif dalam komunikasi email?

## 1.3. Ruang Lingkup Masalah

Dalam sebuah penelitian, perlu diberi batasan masalah agar pembahasan yang dibahas nantinya tidak meluas atau keluar dari topik permasalahan yang disingkat sehingga dapat berfokus dan tepat sasaran. Ruang lingkup permasalahan pada penelitian ini adalah sebagai berikut :

1. Penelitian ini akan membahas penerapan algoritma Advanced Encryption Standard (AES) dalam konteks email di Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo. Fokus akan diberikan pada proses enkripsi dan dekripsi data, serta bagaimana metode ini dapat meningkatkan kerahasiaan dan integritas informasi yang dikirimkan melalui email.
2. Menganalisis tantangan utama yang dihadapi oleh Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo dalam melindungi data sensitif dari akses yang tidak sah dalam email. Ruang lingkup ini akan mencakup tantangan teknis, kebijakan internal, serta kesadaran dan pelatihan pengguna terkait keamanan informasi. Penelitian ini tidak akan membahas aspek keamanan data di luar konteks email, seperti keamanan sistem informasi secara keseluruhan atau aplikasi lain yang tidak terkait.
3. Metode yang digunakan pada penelitian ini adalah Advanced Encryption Standard (AES) 256 Bit.

## 1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Untuk menganalisis penerapan metode kriptografi, khususnya algoritma Advanced Encryption Standard (AES), dalam sistem email di Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo. Penelitian ini bertujuan untuk mengevaluasi bagaimana penerapan AES dapat meningkatkan kerahasiaan dan integritas informasi yang dikirimkan melalui email.

2. Mengidentifikasi tantangan yang dihadapi oleh Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo dalam melindungi data sensitif, serta memberikan rekomendasi berdasarkan hasil analisis penerapan AES. Rekomendasi ini diharapkan dapat membantu dalam meningkatkan sistem keamanan informasi mereka.

## 1.5. Manfaat Penelitian

Manfaat yang diharapkan dari pelaksanaan penelitian ini antara lain sebagai berikut:

1. Manfaat Teoritis :

   Penelitian ini diharapkan dapat memperkaya literatur mengenai penerapan algoritma Advanced Encryption Standard (AES) dalam pengamanan data, khususnya pada email. Hasil penelitian ini juga dapat menjadi referensi bagi pengembangan metode kriptografi lainnya untuk meningkatkan keamanan informasi di era digital.

2. Manfaat Praktis :
   - Bagi Dinas Kominfotik Provinsi Gorontalo: Penelitian ini diharapkan dapat memberikan wawasan dan rekomendasi praktis bagi Dinas Komunikasi dan Informatika (Kominfotik) Provinsi Gorontalo dalam menerapkan metode kriptografi, khususnya algoritma Advanced Encryption Standard (AES). Dengan penerapan yang tepat, diharapkan dapat meningkatkan keamanan dan kerahasiaan informasi dalam email, sehingga melindungi data sensitif dari akses yang tidak sah.
   - Bagi Instansi Pemerintah Lainnya: Hasil penelitian ini dapat menjadi acuan bagi instansi pemerintah lain untuk menggunakan teknologi kriptografi dalam melindungi data sensitif.