BAB 1
PENDAHULUAN

1.1 Latar Belakang

Email dikenal sebagai salah satu sarana komunikasi paling umum digunakan baik dalam konteks pribadi maupun bisnis. Pesan-pesan yang dikirim melalui *email* dapat berisi informasi rahasia, data pribadi, rincian keuangan, hingga strategi bisnis yang berharga. Jika pesan-pesan ini jatuh ke tangan yang salah, dapat mengakibatkan terjadinya pencurian data, penyalahgunaan identitas, kerugian finansial, atau bahkan merusak reputasi suatu individu atau organisasi.

Telah tercatat sejumlah serangan *cyber* yang menargetkan *email* dan mengakibatkan kerugian pada penggunanya. Misalnya, pada tahun 2017, banyak pengguna *Gmail* di seluruh dunia mengalami *Gmail Phishing Attack* di mana penyerang berpura-pura menjadi suatu organisasi resmi dan mengirimkan *email* agar pengguna memberikan informasi pribadinya. Selain itu, sebuah laporan yang baru-baru ini diterbitkan *Google Threat Analysis Group* (TAG) mengungkapkan bahwa suatu kelompok ancaman spionase yang diyakini mendapat dukungan dari pemerintah Iran memiliki alat baru yang dikenal sebagai *hyperscrape* yang telah berhasil digunakan untuk meretas sejumlah kecil akun pengguna *Gmail*.

Mengambil contoh dalam kehidupan sehari-hari, saat akan membuat akun sosial media seperti *facebook*, *instagram*, atau akun *market place* seperti Tokopedia atau Shopee, pengguna diminta mengaitkan akun-akun tersebut dengan *email* dan diwajibkan mencentang persetujuan kebijakan privasi, dan pengguna biasanya melakukannya tanpa membaca terlebih dahulu apa saja yang ada dalam persetujuan tersebut. Ternyata pada syarat-syarat tersebut salah satunya dapat berisi persetujuan agar suatu pihak ketiga dapat melihat isi pesan *email*. Oleh karena itu, diperlukan tindakan pengamanan untuk mengirim pesan-pesan rahasia melalui *email* untuk mencegah akses yang tidak diinginkan. Dalam hal ini, kriptografi memegang peranan yang penting.

Kriptografi adalah ilmu mengenai bagaimana mengubah pesan sehingga seseorang yang memiliki akses ke pesan tersebut tidak bisa membacanya tanpa algoritma dan kunci yang sesuai (Easttom, 2021). Dalam kriptografi terdapat istilah enkripsi, dekripsi, plainteks, cipherteks, dan kunci. Enkripsi adalah proses

penyandian dari pesan yang dapat dimengerti (plainteks) menjadi sebuah pesan tersamar (cipherteks), sementara dekripsi adalah proses mengembalikan cipherteks menjadi plainteks, hal ini biasa dilakukan oleh penerima yang dituju.

Kriptografi dibagi menjadi dua jenis berdasarkan jumlah kunci yang digunakan pada enkripsi dan dekripsinya, yaitu algoritma kriptografi simetris dan asimetris. Dalam kriptografi simetris terdapat kunci yang sama yang digunakan untuk enkripsi dan dekripsi, sementara dalam kriptografi asimetris digunakan kunci yang berbeda untuk mengenkripsi dan dekripsi data, yakni kunci publik dan kunci privat (Munir, 2006).

Dalam penerapannya terdapat beberapa kekurangan baik pada algoritma asimetris maupun algoritma simetris. Pada algoritma simetris, kunci yang sama digunakan untuk enkripsi dan dekripsi, masalah timbul ketika diperlukannya tahap mendistribusikan kunci tersebut secara aman ke pihak lain. Sedangkan pada algoritma asimetris, proses yang dibutuhkan untuk enkripsi dan dekripsi cenderung lebih lambat dibandingkan pada algoritma simetris (Basri, 2016).

Untuk mengatasi kekurangan pada algoritma asimetris dan simetris, maka akan digunakan kriptografi *hybrid* yang merupakan kombinasi dari algoritma simetris dan asimetris di mana kunci simetris akan dienkripsi menggunakan kunci asimetris sehingga pengiriman kunci simetris lebih aman. Dalam hal ini, algoritma kriptografi yang dipilih adalah algoritma RSA yang ditingkatkan (asimetris) dan algoritma AES (simetris).

Algoritma Rivest Shamir Adleman (RSA) merupakan kriptografi asimetris yang menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Algoritma RSA terkenal akan keamanannya yang kuat didasarkan pada sulitnya operasi eksponensial dan faktorisasi suatu bilangan menjadi dua bilangan prima. Namun sejak tahun 2002 hingga kini sudah ditemukan metode kriptanalisis untuk memecahkan algoritma ini diantaranya metode *Lattice*, *Hastad's Attack*, *Coppersmith's Attack*, dan *Wiener's Attack*. Berdasarkan hal tersebut, digunakan algoritma kriptografi RSA yang telah ditingkatkan agar kemungkinan kriptanalisis dapat diminimalisir (Mufadilah, 2019).

Kriptografi *Advanced Encryption Standard* (AES) merupakan standar kriptografi pengganti *Data Encryption Standard (DES)* yang dihasilkan dari

sayembara terbuka oleh *National Institute of Standards and Technology (NIST)* pada tahun 1997. AES menggunakan algoritma simetrik dalam proses enkripsi dan dekripsinya. Basri (2016) mengemukakan bahwa metode simetris cenderung membutuhkan waktu komputasi yang lebih cepat dibandingkan metode asimetris, Anwar dkk. (2018) juga menemukan bahwa performa algoritma AES jauh lebih cepat dibanding RSA dengan rata-rata kurang lebih 236x lebih cepat saat proses enkripsi dan 2,5x lebih cepat pada saat dekripsi.

Terdapat beberapa penelitian sebelumnya yang mengkaji mengenai RSA dan AES. Hermawan dan Ujianto (2021) pada penelitian yang berjudul "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA" mengimplementasikan algoritma RSA dan AES pada proses enkripsi dan dekripsinya. Dalam penelitian tersebut belum diterapkan algoritma RSA yang ditingkatkan, dan penerapannya pada aplikasi *email*. Pada algoritmanya pula, terdapat tahapan transmisi kunci privat yang seharusnya menjadi rahasia. Ferdinan (2021) sudah mengimplementasikan algoritma kriptografi pada aplikasi pengiriman *email*, dalam hal ini algoritma kriptografi yang digunakan adalah *Elliptic Curve Diffie Helman*. Bimantoro dan Sari (2021) menyimpulkan bahwa gabungan metode kriptografi RSA dan AES menghasilkan performa yang baik dan dapat memproses data dalam jumlah besar dalam waktu milisekon. Namun, disebutkan pula bahwa dalam pengujiannya desain yang diajukan masih belum sempurna dan dapat ditingkatkan lagi performa dan keamanannya.

Berdasarkan penjabaran di atas, dapat diketahui bahwa sudah ada beberapa penelitian mengenai penggabungan RSA dan AES. Namun, algoritma RSA yang dipakai merupakan algoritma dasar RSA. Pada penelitian ini, penulis akan menggabungan metode kriptografi RSA yang ditingkatkan dan kriptografi AES untuk diaplikasikan pada pengirim *email*. Dengan demikian, dapat disimpulkan bahwa penelitian yang akan dilakukan masih tergolong baru dan belum dilakukan oleh peneliti terdahulu.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka permasalahan yang dirumuskan adalah:

1. Bagaimana skema algoritma kriptografi RSA yang ditingkatkan dan AES pada aplikasi pengirim *email*?

2. Bagaimana konstruksi program aplikasi pengirim *email* menggunakan penggabungan algoritma kriptografi RSA yang ditingkatkan dan AES?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang sistem penggabungan algoritma kriptografi RSA yang ditingkatkan dan AES untuk aplikasi pengirim *email.*
2. Membuat aplikasi pengirim *email* menggunakan gabungan algoritma kriptografi RSA yang ditingkatkan dan AES.

1.4 Batasan Penelitian

Adapun pembatasan masalah dalam penelitian ini adalah sebagai berikut.

1. Jenis Kriptografi AES yang digunakan adalah AES-128.
2. Dalam penggunaan program aplikasi pengirim *email*, program masih terbatas hanya untuk pengiriman pesan antara *email* yang dapat mengizinkan pihak ketiga untuk mengiriman *email*. *Email* yang memenuhi kriteria ini adalah Google *Mail* dan *Yahoo Mail*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut.

1. Manfaat teoritis

   Secara teoritis hasil penelitian ini diharapkan dapat memberi kontribusi dalam bidang matematika terapan melalui pengembangan kriptografi khususnya dalam algoritma kriptografi RSA dan AES.

2. Manfaat praktis

   Secara praktis hasil penelitian ini diharapkan dapat bermanfaat berupa aplikasi hasil implementasi penggabungan metode kriptografi RSA yang ditingkatkan dan kriptografi AES yang digunakan untuk pengiriman *email*.