BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi enkripsi sangat penting saat ini untuk melindungi dan menjamin kerahasiaan sebuah data, baik itu data pribadi maupun data organisasi. Dalam dunia kriptografi, terdapat berbagai macam jenis metode dan algoritma yang dapat digunakan untuk mengenkripsi sebuah data. Dalam konteks perlindungan dan kerahasiaan sebuah data organisasi atau instansi, diperlukan metode enkripsi yang efektif untuk menjamin keamanan dan kerahasiaan data.

Dalam penerapannya, kriptografi memiliki tujuan untuk memberi layanan keamanan, diantaranya kerahasiaan, integritas data, otentikasi, dan penyangkalan. Semua tujuan itu ialah agar menciptakan rasa aman dan nyaman setelah memberikan data yang bersifat rahasia. Enkripsi adalah teknik mengamankan data dengan isi dari informasi atau data (*Plaintext*) kedalam sandi (*Ciphertext*) yang hanya dapat dibuka atau di dekripsi oleh yang diketahui oleh pengirim atau yang sudah memiliki izin untuk memiliki kunci. Dekripsi adalah teknik untuk mengkonversikan sandi (*Ciphertext*) pada file yang telah di enkripsi kedalam teks biasa (*Plaintext*) atau bahasa manusia dengan menggunakan kunci yang telah dibuat oleh pengirim.

Kriptografi memiliki 3 jenis algoritma yang berbeda berdasarkan kuncinya, yaitu Algoritma Kunci Simetris (*Symmetric Key*), Kunci Asimetris (*Asymetric Key*), dan fungsi *Hash*. Pada algoritma kunci simetris yang umumnya digunakan ialah DES, RIJNDAEL, dan Blowfish. Pada algoritma kunci asimetris yang umumnya digunakan ialah *Diffie-Hellman*, RSA, DSA dan ElGamal. Pada algoritma fungsi *Hash* yang umumnya digunakan ialah MD-5, SHA-256, dan MAC.

Kaggle ialah salah satu situs penyedia *open-source database* untuk selanjutnya digunakan oleh peneliti yang membutuhkan sumber data sebagai bahan penelitian mereka. Terdapat banyak topik yang dapat ditemukan dan

digunakan secara bebas dan terbuka dengan melihat kegiatan peneliti yang sudah menggunakan data tersebut untuk selanjutnya mereka kembangkan dari penelitian sebelumnya atau yang sudah ada. Salah satu data yang dapat digunakan dari situs tersebut ialah ialah *database* citra digital medis penyakit COVID-19 dimana berisi citra atau gambar hasil MRI pasien yang terkena dampak dari penyakit tersebut.

Karena penerapan data asli khususnya adalah data gambar, maka terdapat masalah keamanan yang menjadi salah satu aspek terpenting dari sistem informasi dengan perkembangan teknologi yang terjadi dan jumlah pertukaran informasi per detik di Internet. Hal ini menyebabkan terjadinya pencurian informasi oleh pihak yang tidak bertanggung jawab. Apabila menyangkut hal-hal yang bersifat pribadi dan rahasia penting untuk diperhatikan keamanannya, maka salah satu upaya untuk mengamankan data berupa citra berwarna adalah dengan menerapkan algoritma kriptografi RSA dan elgamal untuk mengkodekan dan mendekode citra.

Dari permasalahan yang ada, penelitian ini akan menunjukkan penerapan tujuan dari kriptografi pada aspek integritas data (*data integrity*) dan kesediaan (*availability*) dengan meneliti perbandingan algoritma kriptografi yang lebih efektif antara algoritma *Rivest–Shamir–Adleman* (RSA) dan ElGamal pada citra digital medis COVID-19.

1.2. Rumusan Masalah

Dari latar belakang yang telah dijelaskan, permasalahan yang akan dibahas adalah :

1) Apakah citra digital dapat di enkripsi oleh algoritma RSA dan ElGamal serta di dekripsi kembali menjadi sesuai dengan citra aslinya?
2) Berdasarkan aspek kesediaan, berapa lama waktu yang diperlukan untuk melakukan enkripsi dan dekripsi dengan kedua algoritma tersebut? Mana yang lebih cepat dan efisien?
3) Berdasarkan aspek kesediaan, berapa ukuran yang dihasilkan setelah melakukan enkripsi dengan kedua algoritma tersebut? Mana yang lebih kecil dan efisien?

4) Berdasarkan aspek integritas data, Bagaimana kualitas data citra sebelum enkripsi dan sesudah dekripsi dengan melihat perbedaan nilai Checksum dan nilai Histogram? Apakah sama atau berbeda?

1.3.Tujuan

Tujuan dari penelitian ini adalah untuk menganalisis perbandingan algoritma yang paling efektif antara algoritma *Rivest–Shamir–Adleman* (RSA) dengan algoritma ElGamal dalam mengenkripsi database citra digital medis COVID-19 yang didapate dari situs *Open-Source* Kaggle dan melihat perbedaan kualitas yang terjadi sebelum enkripsi dan dan sesudah dekripsi.

1.4.Manfaat Penelitian

Manfaat dari penelitian ini adalah :

a. Bagi Publik : dapat memahami pentingnya keamanan dan kerahasiaan data dan mengetahui algoritma yang lebih efektif dengan membandingkan algoritma kriptografi antara RSA dan ElGamal untuk mengamankan data citra digital medis COVID-19.
b. Bagi Peneliti : dapat menerapkan ilmu yang telah didapat, memahami lebih dalam tentang algoritma enkripsi RSA dan ElGamal pada data citra digital medis.

1.5.Batasan Masalah

Sedangkan permasalahan yang dibahas, terbatas pada beberapa pembahasan sebagai berikut :

a. Simulasi enkripsi menggunakan algoritma kriptografi RSA dan Elgamal menggunakan Bahasa pemrograman Python
b. Data rekam digital medis COVID-19 menggunakan citra MRI dengan format .JPG dan .JPEG dari https://www.kaggle.com/datasets/edoardovantaggiato/covid19-xray-two-proposed-databases .
c. Perbandingan efektifitas dilihat berdasarkan aspek kecepatan proses enkripsi dan dekripsi, integritas citra Checksum SHA256 menggunakan aplikasi pihak ketiga https://emn178.github.io/online-tools/sha256_checksum.html dan perbandingan nilai Histogram dari citra asli dengan citra hasil

dekripsi kedua algoritma menggunakan aplikasi pihak ketiga https://www.dcode.fr/image-histogram .

1.6.Luaran yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah mengetahui keefektifan dari algoritma RSA dan ElGamal berdasarkan aspek yang telah disebutkan pada batasan masalah.

1.7.Sistematika Penulisan

Sistematika penulisan dari skripsi ini sendiri terdiri dari beberapa bagian utama yakni sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini berisi tentang Latar Belakang, Tujuan Penelitian, Manfaat Penelitian, Rumusan Masalah, Batasan Masalah, Luaran yang Diharapkan, dan Sistematika Penulisan dari penelitian ini.

BAB 2 LANDASAN TEORI

Pada bab ini berisi tentang teori – teori mendasar yang digunakan dalam penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini menjelaskan beberapa metode penelitian yang digunakan oleh penulis, urutan tahap-tahapannya dalam melakukan penelitian secara keseluruhan, alat bantu yang digunakan, dan gambaran garis waktu penelitian yang dilakukan mulai dari identifikasi masalah hingga evaluasi penelitian selesai.

BAB 4 PEMBAHASAN

Pada bab ini menjelaskan mengenai analisa dan perancangan sistem enkripsi yang di teliti serta algoritma dan bentuk sistem yang digunakan sesuai dengan rumusan masalah, landasan teori dan metodologi penelitian yang akan diteliti

BAB 5 KESIMPULAN

Pada bab ini berisi kesimpulan dari hasil Analisa yang telah dilakukan serta saran yang dapat digunakan untuk pengembangan pada penelitian selanjutnya

DAFTAR PUSTAKA

LAMPIRAN