BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Kemudahan dalam bertukar informasi merupakan salah satu dampak positif dengan adanya teknologi internet. Setiap harinya, jutaan orang mengirimkan pesan berupa gambar melalui internet. Sebuah gambar atau citra dapat memiliki informasi yang sensitif. Jika citra yang memiki informasi sensitif jatuh kepada pihak yang tidak bertanggungjawab, tentunya merupakan hal yang fatal. Informasi tersebut dapat dimanipulasi atau dirubah sehingga mempengaruhi keaslian dan keabsahan file tersebut. Citra rekam medis merupakan contoh salah satu citra yang memiliki informasi sensitif. Peraturan Menteri Kesehatan Republik Indonesia Nomor 269/MENKES/PER/III/2008 tentang Rekam Medis menjelaskan bahwa yang dimaksud dengan rekam medis adalah berkas yang berisikan catatan dan dokumen tentang identitas pasien, pemeriksaan, pengobatan, tindakan dan pelayanan lain yang telah diberikan kepada pasien. Karena berisi informasi yang merupakan privasi dari pasien, diperlukan perhatian khusus pada kerahasiaan dan keamanan dari citra medis. Hal ini tentunya menjadi tantangan bagi tenaga kesehatan pada saat ini. Tenaga kesehatan dituntut untuk menjaga kerahasiaan, keamanan, dan keaslian citra rekam medis dari pihak yang tidak berhak disaat teknologi semakin maju.

Analisis selama 6 bulan yang dilakukan oleh *CyberAngle* terhadap 4,3 milyar alamat IP menemukan bahwa terdapat 45 juta file citra medis yang dapat diakses secara bebas pada 2.140 lebih server yang tidak terlindungi di 67 negara. Analis mengatakan bahwa file citra medis yang dapat diakses secara bebas mengandung metadata yang berisi informasi pasien seperti nama, tanggal lahir, alamat, dan lain – lain serta informasi kesehatan seperti tinggi, berat, diagnosis dan lain – lain (*CyberAngle*, 2020). Berdasarkan laporan hasil analisis tersebut, metode penyimpanan atau pengiriman file citra medis yang dilakukan saat ini masih belum cukup baik. File citra medis dapat diakses secara mudah dan dapat dimanfaatkan untuk hal – hal yang negatif. Untuk menyelesaikan permasalahan tersebut, dapat dilakukan pengamanan file citra medis menggunakan teknik kriptografi.

Kata kriptografi berasal dari Bahasa Yunani, *crypto* yang memiliki arti rahasia dan *graphia* memiliki arti tulisan. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Ariyus, 2008). Kriptografi merupakan ilmu dan seni yang ditujukan untuk menjaga kerahasiaan pesan dengan cara menyamarkannya ke bentuk yang tidak dapat dipahami lagi artinya (Meyer, 1982). Enkripsi merupakan proses penyandian menggunakan kode atau algoritma tertentu dari pesan asli yang dapat dipahami (*plaintext*) menjadi pesan yang tidak dipahami (*chipertext*). Dekripsi merupakan proses perubahan pesan menggunakan kode atau algoritma tertentu dari *chipertext* menjadi *plaintext* agar pesan tersebut dapat dipahami oleh penerima.

Berdasarkan kuncinya, algoritma kriptografi terbagi menjadi dua, yaitu algoritma simetri (*symmetry algorithm*) dan algoritma asimetri (*asymmetry algoritm*) (Munir, 2019). *Advanced Encryption Standard* (AES) merupakan salah satu contoh dari algoritma simetri. *National Institute of Standard and Technology* (NIST) merilis algoritma AES untuk menggantikan algoritma *Data Encryption Standard* (DES) pada tahun 2001. Algoritma AES merupakan algoritma yang memiliki proses yang cepat dan kuat (Amalia dkk, 2018). Sebagai algoritma simetri, AES memiliki kelemahan pada kuncinya. Algoritma simetri menggunakan kunci yang sama saat melakukan proses enkripsi dan dekripsi. Apabila ada orang lain yang mengetahui kunci yang digunakan, bukan tidak mungkin data tersebut dapat didekripsi sehingga data tersebut menjadi tidak rahasia lagi.

Permasalah tersebut dapat diatasi dengan memanfaatkan algoritma ElGamal. Algoritma ElGamal merupakan salah satu contoh dari algoritma asimetri. Algoritma asimetri memiliki dua kunci yang berbeda. Kunci yang digunakan pada proses enkripsi bersifat publik atau tidak rahasia. Siapapun dapat mengetahui kunci publik. Berbeda dengan kunci yang digunakan saat enkripsi, kunci yang digunakan saat dekripsi merupakan kunci rahasia. Kunci tersebut hanya diketahui oleh penerima pesan.

Pada penelitian ini, penulis akan menganalisis penggunaan algoritma *Advanced Encryption Standard* (AES) pada citra medis serta algoritma ElGamal

pada pengamanan kunci yang digunakan saat enkripsi dan dekripsi. Diharapkan, dengan kombinasi antara algoritma simetri dan algoritma asimetri tersebut dapat meningkatkan keamanan dan kerahasiaan pada citra medis

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah disampaikan, permasalahan yang akan dibahas adalah :

1. Bagaimana cara mengamankan file citra medis agar hanya orang yang berhak saja yang mengetahuinya?
2. Apa saja tahap yang harus dilakukan untuk mengamankan citra medis?
3. Bagaimana kualitas citra medis setelah melalui proses pengamanan?

1.3 Batasan Masalah

Untuk mempersempit pembahasan pada skripsi ini, maka dibuat batasan-batasan sebagai berikut:

1. File citra medis digital yang digunakan berupa citra MRI dengan format BMP.
2. Algoritma yang diterapkan pada saat enkripsi dan dekripsi file citra medis digital adalah algoritma *Advanced Encryption Standard* (AES).
3. Algoritma ElGamal diterapkan pada kunci yang digunakan pada saat enkripsi dan dekripsi file citra medis digital.
4. Bahasa pemrograman yang digunakan pada pembuatan aplikasi adalah Python.
5. Penelitian ini tidak membahas kelebihan dan kekurangan pada setiap mode operasi blok cipher yang digunakan.
6. Peneliti befokus pada implementasi dan analisis dari program yang dihasilkan, bukan pada pembuatan program.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam pembuatan laporan skripsi ini adalah sebagai berikut :

1. Melakukan proses enkripsi dan dekripsi pada citra medis menggunakan kombinasi algoritma AES dengan algoritma Elgamal.
2. Mengetahui apakah kombinasi algoritma AES dengan algoritma Elgamal dapat meningkatkan keamanan dari citra medis.
3. Mengetahui kualitas citra medis setelah melalui proses enkripsi dan dekripsi.

1.5 Sistematika Penulisan

Sistematika penulisan dalam pembuatan skripsi ini adalah sebagai berikut :

Bab I Pendahuluan, bab ini menjelaskan tentang latar belakang pembuatan skripsi, rumusan dan batasan masalah dalam penelitian, tujuan dan sistematika penulisan dalam penulisan skirpsi.

Bab II Landasan Teori, bab ini menjelaskan tentang penelitian sebelumnya yang mengkaji tentang enkripsi pada citra digital. Selain itu, bab ini juga menjelaskan pengertian permasalahan yang dibahas pada skripsi ini, meliputi Pengertian Kriptografi, Blok Cipher, Mode Operasi, Algoritma *Advanced Encryption Standard* (AES), Algoritma Elgamal, Citra Digital, dan Citra Medis MRI,.

Bab III Metodologi Penelitian, bab ini membahas tentang metodologi dan tahapan-tahapan yang digunakan oleh penulis dalam menyelesaikan penelitian ini.

Bab IV Pembahasan, bab ini membahas implementasi dari sistem yang telah dirancang dan pengujian terhadap sistem tersebut untuk mengetahui apakah sistem tersebut dapat menyelesaikan permasalahan yang ada.

Bab V Penutup, bab ini berisi hasil dari penelitian yang telah dilakukan dalam bentuk kesimpulan dan saran.