BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan data menjadi salah satu kubutuhan yang harus dipenuhi saat ini. Efek dari perkembangan teknologi ialah akses terhadap suatu informasi akan lebih mudah. Hal ini berpengaruh pada keamanan dan integritas data. Salah satu jenis data pribadi yang termasuk bersifat sensitif adalah data - data medis. Bagaimana yang tertulis dalam Undang -undang Nomor 29 tahun 2004 Pasal 46 ayat 1, berkas yang berisi dokumen dan catatan terkait identitas pasien, pemeriksaan, tindakan, pelayanan, dan pengobatan yang diterapkan kepada pasien merupakan sebuah rekam medis. (Indonesia, Undang-Undang, 2004). Sedangkan pada Manual Rekam Medis Konsil Kedokteran Indonesia, dijelaskan lebih lanjut bahwa dokumen yang termasuk kedalam rekam medis adalah hasil foto rontgen dan hasil laboratorium lainnya (Konsil Kedokteran Indonesia 2006, hlm.3). Salah satu bentuk dari hasil laboratorium selain citra rontgen adalah citra MRI (*Magnetic Resonance* Imaging). Dari data tersebut dapat terdeteksi kondisi tubuh pasien dengan lebih detail. Agar data – data yang terdapat dalam citra MRI tersebut tidak diketahui dan kemudian digunakan oleh pihak – pihak yang tidak berkepentingan, maka dibutuhkan sebuah langkah pengamanan terhadap citra tersebut. Salah satu bentuk pengamanan citra yang dapat digunakan pada citra medis adalah dengan teknik kriptografi.

Terdapat dua tipe algoritma kriptografi jika dilihat dari persamaan kunci, yaitu algoritma simetrik (*symmetric algorithm*) dan algoritma asimetrik (*asymmetric algorithm*). Salah satu contoh algoritma kriptografi simetrik adalah *Advanced Encrption Standard* (AES), algoritma ini memiliki kunci dekripsi yang sama dengan kunci enkripsi dengan pilihan panjang kunci 128bit, 192 bit, atau 256 bit (Kromodimoeljo 2010, hlm.104). Pada penelitian yang berjudul “Studi Algoritma Rijndael Dalam Sistem Keamanan Data”, menyimpulkan bahwa AES sangat aman untuk

melindungi data, karena panjang kunci dan variatif pada kunci AES bisa mencegah dari segala macam ancaman (Eko Satria, 2009). Namun, terdapat kelemahan dalam algoritma jenis simetris yaitu pada kunci yang digunakan pada proses enkripsi dan dekripsi merupakan kunci yang sama. Maka dari itu perlu diamankannya kunci dari algoritma AES tersebut. Salah satu algoritma yang dapat digunakan untuk mengamankan kunci dari AES adalah algoritma Diffie-Hellman. Algoritma ini sering digunakan sebagai sebagai pengaman pada proses pertukaran kunci. Algoritma Diffie-Hellman akan menghasilkan kunci baru yang nanti akan dikombinasikan dengan algoritma AES.

Pada penelitian ini, algoritma Diffie-Hellman akan menghasilkan kunci yang nanti akan dikombinasikan dengan kunci enkripsi dari algoritma AES. Kemudian, citra akan di enkripsi menggunakan algoritma AES dengan kunci hasil dari kombinasi yang sudah dilakukan sebelumnya.

Penelitian ini akan menganalisis tingkat keberhasilan pengamanan citra digital medis menggunakan kombinasi algoritma AES sebagai enkripsi lapis pertama dan kemudian algoritma Diffie-Hellman sebagai pengamanan lanjutan pada proses pertukaran dan pembangkitan kunci. Kombinasi dua jenis algoritma ini diharapkan mampu memenuhi aspek keamanan dan kerahasiaan yang dibutuhkan oleh citra digital medis.

1.2. Rumusan Masalah

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

1. Apakah proses enkripsi menggunakan algoritma AES dapat mengamankan file citra digital medis?
2. Apakah kombinasi algoritma pertukaran kunci Diffie-Hellman data dapat meningkatkan keamanan kunci enkripsi dari algoritma AES?
3. Bagaimana kualitas citra sebelum dan sesudah melalui proses enkripsi dan dekripsi?

1.3. Batasan Masalah

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

a. File citra digital medis yang digunakan berupa citra MRI dengan format file JPG dan JPEG.
b. Algoritma AES diterapkan pada proses enkripsi dan dekripsi file citra digital medis.
c. Algoritma Diffie-Hellman diterapkan pada proses pengamanan pertukaran dan pembangkitan kunci yang digunakan pada proses enkripsi dan dekripsi file citra digital medis.

1.4. Tujuan dan Manfaat

Tujuan penelitian ini adalah untuk mengembangkan suatu sistem pengamanan citra digital medis menggunakan kombinasi algoritma AES pada proses enkripsi-dekripsi data dan algoritma Diffie-Hellman pada proses pertukaran dan pembangkitan kunci.

1.5. Manfaat Penilitan

Manfaat dari penelitian ini adalah sebagai berikut :

a. Untuk Pasien

   Menjadi solusi pengamanan citra digital medis menggunakan kombinasi algoritma AES dan Diffie-Hellman sehingga dapat memenuhi kebutuhan akan keamanan dan kerahasiaan citra digital medis.

b. Untuk Penulis

   Meningkatkan pengetahuan dan wawasan dengan menerapkan ilmu pengetahuan di bidang kriptografi mengenai algoritma AES dan Diffie-Hellman.

1.6. Ruang Lingkup

Ruang lingkup dari penelitian yang dilakukan adalah mengenai kombinasi algoritma AES pada proses enkripsi dan deksripsi data dan algoritma Diffie-Hellman dalam proses pertukaran kunci enkripsi terhadap pengamanan citra digital medis yang memiliki tipe file .JPG dan .JPEG.

1.7. Luaran yang Diharapkan

Luaran yang diharapkan pada penelitian ini adalah mengetahui tingkat keberhasilan pengamanan citra digital medis dengan proses enkripsi dan

dekripsi menggunakan algoritma AES yang dikombinasikan dengan algoritma Diffie-Hellman pada proses pembentukan kunci enkripsi.

1.8. Sistematika Penulisan

Sistematika penulisan yang digunakan pada penelitian ini diatur dan disusun dalam lima bab dan daftar pustaka yang dibagi menjadi beberapa sub bab di dalamnya, dengan sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

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

BAB 2 LANDASAN TEORI

Bab ini berissi tentang teori – teori mendasar yang digunakan dalam penelitian ini.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini menjelaskan beberapa metode penelitian yang digunakan oleh penulis dan urutan tahap-tahapannya dalam melakukan penelitian secara keseluruhan.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini membahas tentang penerapan Algoritma FP-Growth dan hasil pola pembelian yang didapat dari analisa keranjang pasar dengan Algoritma FP-Growth tersebut.

BAB 5 PENUTUP

Bab ini berisikan kesimpulan dan saran dari hasil dan pembahasan yang di tulis pada bab 4 (empat) selama proses penelitian sebagai acuan pada penelitian yang selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN