BAB I
PENDAHULUAN

A. LATAR BELAKANG

Perkembangan teknologi informasi dan komunikasi saat ini, mengakibatkan manusia dapat berkomunikasi dan saling bertukar data dan informasi tanpa dihalangi oleh jarak dan waktu. Seiring dengan tuntutan akan keamanan untuk kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat menimbulkan tuntutan tersedianya suatu sistem pengamanan data dan informasi yang lebih baik agar dapat mengamankan data dari berbagai ancaman. Berkembangnya cabang ilmu yang mempelajari tentang cara-cara pengamanan data merupakan dampak positif dari tuntutan tersedianya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi. Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan nama Kriptografi.

Keamanan (*security*) pada komputer menjadi isu penting pada era teknologi ini. Banyak kejahatan *cyber* yang pernah kita dengar dari media masa mengancam kemanan sistem. Pelaku kejahatan memanfaatkan celah kemanan yang ada untuk dimasuki dan melakukan manipulasi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta autentifikasi (Munir, 2006).

Kriptografi merupakan salah satu komponen yang tidak dapat diabaikan dalam membangun keamanan komputer. Peran utama kriptografi untuk mengamankan data atau dokumen dengan menggunakan teknik enkripsi, sehingga data dan dokumen tidak bisa dibaca oleh orang yang tidak berhak. Pemalsuan pesan dan dokumen juga dapat dibuktikan sehingga orang yang mengirim pesan tidak bisa mengelak dari tanggungjawab telah mengirim pesan

tersebut. Enkripsi (*encryption*) merupakan proses menyandikan plainteks menjadi cipherteks.

Kriptografi AES merupakan standart kriptografi baru yang di buat untuk menggantikan standart enkripsi kriptografi yang lama yaitu DES (Data *Encryption Standard*). AES menggunakan Algoritma yang di temukan oleh Vincent Rijmen dan Joan Daemen yang berasal dari belgia yang memberikan nama algoritmanya Rijndael di baca Rhine-doll. Rijndael mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Panjang kunci dan ukuran blok pada AES dapat dipilih secara independen. Karena AES mempunyai panjang kunci paling sedikit 128 bit, maka AES tahan terhadap serangan *exhaustive key search* dengan teknologi saat ini. Panjang kunci 128 bit, maka terdapat sebanyak 12128 = 3,4 x 1038 Jika digunakan komputer tercepat yang dapat mencoba 1 juta kunci setiap detik, maka akan dibutuhkan waktu 5,4 x 1024 tahun untuk mencoba seluruh kemungkinan kunci sampai kunci tersebut bisa di temukan.

Masalah keamanan komputer dan kerahasiaan data merupakan sesuatu yang sangat penting dalam era informasi ini. Keamanan data pada komputer tidak hanya bergantung pada firewall dan *intrusion detection* system saja, keamanan data dari data itu sendiri merupakan hal yang sangat perlu diperhatikan, jika *firewall* dan perangakat keamanan lainnya bisa di duplikasi oleh orang yang tidak berhak. SAT LANTAS Polres Banyumas salah satunya memiliki data dokumen dan gambar yang penting, penyimpanan data SAT LANTAS Polres Banyumas masih disimpan secara manual rentan terjadi penyadapan data oleh pihak yang tidak bertanggungjawab. Maka perlu adanya kemanan sistem dengan menggunakan metode Kriptografi AES sehingga kemanan data terjamin.

B. RUMUSAN MASALAH

Berdasarkan latar belakang masalah dan identifikasi masalah maka permasalah dalam penelitian dirumuskan sebagai berikut:

1. Bagaimana penerapan kriptografi AES dapat memproteksi *file* dokumen dan gambar sehingga kerahasiaan data dapat terjamin.
2. Bagaimana sistem kriptografi AES dapat mengamankan *file* dokumen dan gambar secara tersembunyi sehingga tidak mudah diretas oleh pihak yang tidak bertanggungjawab.

C. BATASAN MASALAH

Untuk lebih memfokuskan pada permasalahan yang akan diteliti, maka penelitian ini dibatasi sebagai berikut:

1. Sistem ini dirancang hanya untuk mengamankan dokumen dan gambar.
2. Sistem ini digunakan untuk mengimplementasikan algoritma kriptografi AES guna memproteksi dokumen dan gambar dari segala ancaman pihak-pihak yang tidak berwenang.
3. Sistem ini dapat mengamankan dokumen dan gambar dengan menggunakan enkripsi dan dibuka dengan dekripsi.