BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi komunikasi dan informasi yang pesat telah membawa perubahan bagi kehidupan manusia. Salah satu contoh nyata dari perkembangan teknologi komunikasi dan informasi adalah perkembangan internet yang memungkinkan pertukaran data dengan mudah melalui internet tersebut. Berbagai kejahatan teknologi komunikasi dan informasi juga turut berkembang seiring dengan perkembangan teknologi komunikasi dan informasi. Berbagai ancaman dari keamanan komunikasi lewat jaringan telah menjadi perhatian bagi para pengguna internet, seperti interupsi, penyadapan, modifikasi, dan fabrikasi. Tentunya ancaman ini akan berakibat pada data-data yang dikomunikasikan (Sukrisno dan Ema Utami, 2007).

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun komunikasi melalui jaringan. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak (Semuil Tjiharjadi dan Marvin Chandra Wijaya, 2009). Teknik pengamanan data dengan enkripsi dan dekripsi dikenal dengan kriptografi.

Kriptografi adalah ilmu yang mempelajari mengenai cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan melakukan enkripsi dan dekripsi pada informasi tersebut dengan suatu kunci khusus. Informasi yang belum mengalami proses enkripsi disebut *plaintext*, sedangkan informasi yang telah mengalami proses enkripsi disebut *ciphertext*. Berbagai algoritma kriptografi telah diciptakan oleh para ahli kriptografi, namun berbagai usaha untuk memecahkannya tidak sedikit yang membawa keberhasilan. Hal ini mendorong para ahli kriptografi untuk menciptakan algoritma-algoritma baru yang lebih aman. Hingga tahun 1990-an, algoritma kriptografi yang banyak dipakai adalah *Data*

Encryption Standard (DES). DES termasuk dalam algoritma enkripsi yang sifatnya *cipher block*. DES mengubah data masukan menjadi blok-blok 64 bit dan menggunakan kunci enkripsi sebesar 56 bit. Setelah mengalami proses enkripsi maka akan menghasilkan output blok 64 bit. Seiring dengan perkembangan teknologi, kunci DES yang sebesar 56 bit dianggap sudah tidak memadai lagi. Pada tahun 1997, NIST (*National Institute of Standards and Technology*) mengadakan sayembara untuk mencari standar algoritma baru yang akan dinamakan AES (*Advanced Encryption Standard*). Setelah melewati tahap seleksi terdapat 5 calon algoritma AES, yaitu *Serpent*, MARS, *Twofish*, *Rijndael*, dan RC6. Pada bulan Oktober 2000, algoritma *Rijndael* terpilih sebagai AES, dan pada bulan November 2001, algoritma *Rijndael* ditetapkan sebagai AES, dan diharapkan algoritma *Rijndael* menjadi standar kriptografi yang dominan paling sedikit selama 10 tahun (Didi Surian dan Rinaldi Munir, 2006).

Citra digital telah digunakan secara luas dalam berbagai macam proses sehingga perlindungan citra digital dari pihak yang tidak memiliki hak akses menjadi sangat penting (Lala Krikor, dkk., 2009). Pemerintah, militer, badan keuangan, rumah sakit, dan perusahaan swasta telah menggunakan citra digital untuk menyimpan informasi penting, misalnya hasil pemeriksaan pasien (untuk rumah sakit), area geografi (untuk penelitian), posisi musuh (untuk militer), produk baru (untuk perusahaan swasta), status keuangan, dan lain-lain. Hampir semua informasi ini dikumpulkan dan disimpan dalam komputer kemudian dikirimkan melalui jaringan, misalnya internet. Bila informasi penting ini jatuh ke tangan orang yang salah, maka akan menyebabkan hal yang tidak diinginkan, misalnya perang (untuk militer) dan penanganan pasien yang salah (untuk rumah sakit). Hal inilah yang menyebabkan perlindungan citra digital menjadi sangat penting (Jayant Kushwaha dan Bhola Nath Roy, 2010). Penelitian ini akan membangun sebuah perangkat lunak untuk mengimplementasikan algoritma kriptografi *Rijndael* pada citra digital. Algoritma *Rijndael* sendiri dipilih karena telah ditetapkan menjadi standar baru algoritma kriptografi (AES) oleh NIST.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan yang akan dibahas adalah bagaimana mengimplementasikan algoritma kriptografi *Rijndael* untuk enkripsi dan dekripsi pada citra digital.

1.3 Batasan Masalah

Permasalahan yang dibahas pada penelitian ini akan dibatasi pada.

1. Kriptografi yang digunakan adalah kriptografi kunci simetri dengan algoritma *Rijndael* mode ECB dengan ukuran blok 128 bit.
2. Implementasi algoritma kriptografi akan dilakukan untuk enkripsi dan dekripsi citra digital format *file* citra bitmap 24 bit.

1.4 Tujuan Penelitian

Tujuan dari diadakannya penelitian ini adalah membangun sebuah perangkat lunak untuk mengimplementasikan enkripsi dan dekripsi pada citra digital dengan algoritma *Rijndael*.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dapat dicapai melalui penelitian ini adalah :

1. Membantu pemahaman alur kerja kriptografi kunci simetri dengan algoritma *Rijndael*.
2. Perangkat lunak yang dibangun dapat menjadi salah satu alternatif untuk mengenkripsi dan mendekripsi *file* berupa citra digital.

1.6 Metoda Penelitian

Metoda pengembangan perangkat lunak kriptografi ini menggunakan model air terjun yang terdiri dari (Roger Pressman, 2002).

1. Analisis

   Tahap ini meliputi analisis kebutuhan dan analisis sistem. Pada tahap ini dilakukan analisis terhadap hal-hal yang berhubungan dengan pembangunan perangkat lunak, seperti citra digital yang akan digunakan, proses dari

algoritma *Rijndael* untuk enkripsi dan dekripsi pada citra digital, bahasa pemrograman yang akan digunakan, dan lain-lain. Sistem kemudian dimodelkan secara logis berdasarkan kebutuhan.

2. Perancangan Perangkat Lunak

   Pada tahap ini permodelan sistem secara logis dibuat menjadi sebuah rancangan fisik perangkat lunak yang akan dibangun.

3. Implementasi

   Setelah melewati tahap perancangan, rancangan perangkat lunak kemudian direalisasikan. Pembangunan perangkat lunak dilakukan dengan menggunakan bahasa pemrograman Visual Basic 6.0.

4. Pengujian

   Pada tahap ini, perangkat lunak yang telah dibangun kemudian diuji. Pengujian yang dilakukan adalah *black-box testing*.

1.7 Sistematika Penulisan

Untuk memberikan gambaran mengenai isi laporan secara keseluruhan, berikut akan diuraikan secara singkat sistematika penulisan laporan sebagai berikut.

BAB 1 PENDAHULUAN

Latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metoda penelitian, dan sistematika penulisan akan dijelaskan pada bab ini.

BAB 2 LANDASAN TEORI

Pembahasan mengenai dasar teori yang akan dipergunakan dalam penelitian akan diuraikan pada bab ini. Dasar teori yang diberikan mencakup teori kriptografi secara umum, teori tentang algoritma *Rijndael*, dan berbagai teori lain yang berhubungan dengan topik yang dibahas.

BAB 3 ANALISIS DAN PERANCANGAN

Beberapa hal yang akan dibahas pada bab ini, antara lain analisis sistem yang akan dibangun, *data flow diagram* sistem yang akan dibangun, dan rancangan antarmuka sistem yang akan dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Proses pembuatan perangkat lunak, tampilan perangkat lunak yang dibuat, dan hasil pengujian perangkat lunak akan dibahas pada bab ini.

BAB 5 PENUTUP

Bab ini berisi simpulan secara umum dan saran yang membangun untuk masa yang akan datang.