BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan sistem informasi membawa banyak manfaat dalam berbagai bidang seperti pendidikan dan bisnis. Internet memungkin setiap orang untuk saling berkomunikasi dan bertukar informasi dengan cepat dan mudah. Pentingnya informasi dari sebuah pesan seringkali tidak diperhatikan sehingga pesan yang dikirim tidak sampai ke penerima dan berakhir di tangan orang lain yang tidak memiliki kepentingan. Untuk itu diperlukan keamanan data agar informasi yang dikirimkan tidak dapat langsung dibaca oleh orang yang tidak berhak atas data atau informasi tersebut.

Keamanan dokumen merupakan salah satu hal terpenting dalam pertukaran data informasi, terutama di dunia maya dimana banyak terdapat ancaman terhadap proses eksekusi. Salah satu aspek keamanan dokumen adalah keasliannya, bentuk dan isinya harus sesuai dengan maksud pembuatnya. Dalam mengatasi masalah keamanan data informasi, salah satu solusi yang dapat dilakukan adalah diterapkan ilmu kriptografi.

Kriptografi merupakan kajian matematika yang berkaitan dengan aspek keamanan informasi seperti menyembunyikan isi data, mencegah data diubah tanpa sepengetahuan, atau mencegah data digunakan tanpa otorisasi yang tepat. Kriptografi berasal dari bahasa Yunani, yakni *crypto* dan *graphia*. Crypto berarti rahasia (*secret*) dan *graphia* yang berarti tulisan (*writing*). Menurut istilah, kriptografi yaitu ilmu dan seni menjaga keamanan pesan saat dikirim dari satu lokasi ke lokasi lain [1]. Kriptografi merupakan bagian dari cabang matematika yang disebut *cryptology*, yang bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga tidak dapat dibocorkan oleh pihak ketiga yang tidak diinginkan.

Secara umum, berdasarkan kuncinya algoritma kriptografi terbagi menjadi dua jenis yaitu algoritma kriptografi simetris dan algoritma kriptografi asimetris. Perbedaan kedua jenis kunci tersebut terletak pada penggunaan kuncinya [2]. Algoritma simetris adalah algoritma dengan kunci enkripsi dan dekripsi yang sama, sehingga harus benar benar dirahasiakan. Sedangkan algoritma kriptografi asimetris terdiri dari dua kunci yang berbeda yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk proses enkripsi, untuk kunci privat digunakan untuk proses dekripsi. Pada algoritma kunci asimetris, kunci publik tidak perlu dirahasiakan sedangkan untuk kunci privat harus dirahasikan, sehingga faktor ini yang membuat kriptografi asimetris lebih aman [2].

Berbagai jenis algoritma kriptografi dapat diterapkan untuk melindungi data informasi. Salah satunya algoritma terpopuler dalam kriptografi adalah algoritma *Rivest Shamir Adleman* (RSA) yang sampai saat ini sulit untuk dipecahkan. RSA merupakan algoritma kriptografi asimetris yang menggunakan kunci berbeda dalam proses enkripsi dan proses dekripsi. Kunci publik (*public key*) digunakan pada proses enkripsi dan kunci privat (*private key*) digunakan pada proses dekripsi. Proses perumusan RSA didasarkan pada *Teorema Euler*, sehingga menghasilkan kunci publik dan kunci privat yang saling berkorelasi. Jadi meskipun proses enkripsi dan proses dekripsi menggunakan dua kunci yang berbeda, hasilnya tetap benar.

Berdasarkan penjelasan di atas, maka peneliti bermaksud untuk melakukan penelitian yang berjudul, "Analisis dan Perancangan Enkripsi Dokumen Menggunakan Metode *Rivest Shamir Adleman* (RSA) Berbasis *Web*". Harapannya program yang dibangun dapat memudahkan pengguna dalam mengenkripsi dokumen secara aman.

1.2 Rumusan Masalah

Berdasarkan latar belakang, pokok permasalahan dalam penelitian ini adalah bagaimana analisis dan perancangan program enkripsi dan dekripsi dokumen menggunakan metode *Rivest Shamir Adleman* (RSA) berbasis *web*.

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, penulis berusaha untuk tidak memperluas cakupan masalah. Maka pada penulisan skripsi ini hanya mencakup :

1. Metode kriptografi yang digunakan adalah metode *Rivest Shamir Adleman* (RSA).
2. Data yang digunakan untuk enkripsi dengan menggunakan algoritma *Rivest Shamir Adleman* (RSA) berupa *file* pdf.
3. Program yang dibuat merupakan implementasi dari algoritma RSA dengan menggunakan bahasa pemrograman PHP.

1.4 Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini adalah merancang sebuah program enkripsi dan dekripsi dokumen dengan menggunakan metode *Rivest Shamir Adleman* (RSA) berbasis *web*.

1.5 Manfaat Penelitian

Berikut manfaat dari penelitian yang dilakukan adalah sabagai berikut.

1. Dapat memberikan pembelajaran tentang kriptografi terutama algoritma *Rivest Shamir Adleman* (RSA) dalam enkripsi dan dekripsi dokumen.
2. Dapat digunakan sebagai alternatif enkripsi *file* pdf sebelum *file* dikirimkan.
3. Dapat memberikan wawasan baru dalam mengembangkan penelitian serupa pada masa selanjutnya.

1.6 Metode Penelitian

Metode penelitian tugas akhir ini adalah tahapan pengerjaan yang digunakan dalam tugas akhir ini agar lebih fokus. Berikut adalah metode yang digunakan untuk mempersiapkan tugas akhir ini:

1.6.1 Analisis Masalah

Metode ini digunakan untuk menganalisis fenomena yang ada yang menyebabkan penelitian ini dilakukan.

1.6.2 Analisis Kebutuhan

Metode ini digunakan untuk menganalisis apa yang diperlukan dalam pembuatan program, seperti spesifikasi perangkat keras, analisis kebutuhan perangkat lunak, dan prosedur yang digunakan dalam pembuatan program yang dibangun.

1.6.3 Perancangan

Metode ini digunakan untuk merancang program yang dibangun seperti perancangan *flowchart*, perancangan diagram *flow*, perancangan antarmuka pengguna, dan perancangan pengujian.

1.6.4 Implementasi

Metode ini diterapkan pada sistem yang dibangun dengan menggunakan hasil perancangan sistem yang telah dibuat sebelumnya.

1.6.5 Pengujian

Metode pengujian ini digunakan untuk menguji program yang telah dibuat.

1.7 Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini terdiri dari lima bab, masing-masing berisi sub-bab yang memberikan gambaran umum pada setiap bab yang dibahas. Uraian dari bab-bab tersebut adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas masalah umum seperti latar belakang masalah, batasan masalah, tujuam penelitian, manfaat penelitian, metode penelitian, dan sistematika penelitian

BAB II LANDASAN TEORI

Bab ini menjelaskan toeri dasar yang digunakan sebagai sumber atau referensi untuk menjadi dasar dalam melakukan penelitian.

BAB III ANALISIS DAN PERANCANGAN

Bab ini menjelaskan analisis yang dibutuhkan dalam perancangan dan pembangunan sistem yang dibuat.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang implementasi dari sistem yang dibangun, menganalisis kinerja sistem dan menguji sistem yang telah dibuat.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan dari penelitian dan saran yang digunakan untuk membangun sistem yang lebih baik di masa mendatang.