BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi adalah sebuah metode untuk memanipulasi suatu pesan rahasia ke dalam bentuk yang tidak diketahui oleh banyak orang dengan tujuan pesan rahasia tersebut terlindungi dari orang yang tidak berhak mengetahuinya. Maka dari itu, kriptografi dijadikan sebagai salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan, yang akan menyebabkan kerugian bagi pemilik informasi [1]. Khususnya pada sebuah perusahaan, terdapat banyak dokumen penting yang berisi data-data rahasia milik perusahaan yang hanya dapat dilihat oleh pihak tertentu. Dengan adanya kriptografi, maka pertukaran data dapat terjaga keamanan dan kerahasiaannya, sehingga data tersebut tidak jatuh pada pihak yang tidak berwenang dan tidak bertanggung jawab.

Salah satunya pada PT. XYZ, dimana perusahaan ini bergerak dalam bidang penyediaan pelayanan jasa, diantaranya kalibrasi, pengujian material, pelatihan, konsultan manajemen mutu, dan pelayanan jasa *maintenance*. Dimana perusahaan tersebut memiliki data penting seperti data terkait prosedur dan metode kalibrasi, dokumen akreditasi dan sertifikasi, laporan hasil pengujian/kalibrasi pelanggan, informasi tentang pelanggan dan proyek, riset dan pengembangan (R&D) *internal*, dan dokumen penting lainnya. Mengingat data ini tidak boleh diketahui oleh pihak yang tidak berkepentingan, terutama kompetitor, karena bisa merugikan. Oleh karena itu diperlukan sebuah pengamanan data agar pertukaran data pun dapat dilakukan secara aman sehingga terhindar dari pencurian data, untuk ini diperlukan sebuah aplikasi dengan metode yang dapat melindungi data dan informasi yang berada didalamnya. Metode yang dimaksud adalah kriptografi.

Kriptografi terbangun dalam blok-blok tertentu dan hanya bisa dipecahkan dengan sejumlah besar daya komputasi. Kriptografi secara khusus dibedakan ke dalam tiga metode kerja yang berbeda. Ketiganya dikembangkan dengan mempertimbangkan kebutuhan keamanan yang berbeda. Ketiga jenis metode kriptografi tersebut adalah asimetris, simetris, dan homorfik. Kriptografi asimetris merupakan kriptografi kunci berbasis publik yang mengenkripsi dan mendekripsi

data menggunakan dua kunci asimetris kriptografi secara terpisah. Kedua kunci ini dikenal sebagai "*public key*" dan "*private key*" Kriptografi simetris merupakan jenis kriptografi di mana hanya ada satu kunci simetris yang bersifat rahasia dan digunakan untuk mengenkripsi *plaintext* dan mendekripsi *ciphertext.* Kriptografi homomorfik merupakan teknik kriptografi atau enkripsi yang didukung oleh jenis algoritma khusus yang memungkinkan jenis operasi tertentu dilakukan pada *ciphertext* tanpa memerlukan akses ke sebuah kunci rahasia.

Berbagai jenis algoritma kriptografi dapat diterapkan untuk melindungi data dan informasi. Diantaranya adalah algoritma kriptografi RSA dan AES. RSA adalah proses penyandian kunci asimetris yang menggunakan kunci berbeda untuk proses enkripsi dan dekripsi. Kunci publik digunakan untuk proses enkripsi dan kunci *private* digunakan untuk proses dekripsi. Kunci AES (*Advanced Encryption Standard*) adalah nilai rahasia yang digunakan dalam algoritma enkripsi AES untuk mengamankan data. AES adalah salah satu algoritma enkripsi yang paling umum digunakan dalam keamanan komputer dan komunikasi data. Kunci AES terdiri dari serangkaian bit yang ditentukan oleh panjang kunci yang digunakan. Panjang kunci yang umum digunakan dalam AES adalah 128-bit, 192-bit, atau 256-bit. Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanannya.

Dalam praktiknya, AES dan RSA sering digunakan bersama-sama untuk memberikan keamanan yang optimal. AES digunakan untuk enkripsi data yang efisien, sedangkan RSA digunakan untuk pertukaran kunci dan tanda tangan digital. Dengan kombinasi ini, kelebihan keduanya dapat dimanfaatkan untuk mencapai keamanan dan kerahasiaan data yang kuat.

Untuk itu peneliti berupaya mewujudkan implementasi keamanan data pada sebuah perusahaan dengan menggunakan metode enkripsi *Rivest Shamir Adleman* dan *Advanced Encryption Standard* ke dalam suatu aplikasi yang mudah digunakan, dalam skripsi yang berjudul **"Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (*Rivest Shamir Adleman*) dan AES (Advanced Encryption Standard) Berbasis Web".**

1.2 Identifikasi Masalah

Melihat permasalah yang ada, maka masalah pokok yang akan dibahas penulis adalah membuat aplikasi enkripsi untuk menjamin kerahasiaan data dengan menggunakan metode *Rivest Shamir Adleman* dan *Advanced Encryption Standard* berbasis web.

1.3 Tujuan dan Manfaat

Tujuan dari penulisan tugas akhir ini adalah menghasilkan aplikasi pengamanan data menggunakan algoritma RSA (*Rivest Shamir Adleman*) dan AES (*Advanced Encryption Standard*) berbasis web.

Adapun manfaat yang didapat dari penulisan ini adalah sebagai berikut:

1. Bagi penulis, dapat menerapkan atau mengaplikasikan ilmu yang diperoleh di bangku kuliah dalam kehidupan, sehingga ilmu yang dikuasai tidak sekedar teori belaka.
2. Bagi kalangan akademik, diharapkan skripsi ini dapat digunakan sebagai pembanding dengan penelitian sejenis di dunia akademis, serta dapat dipertimbangkan untuk penelitian dan pengembangan lebih lanjut.
3. Bagi kalangan umum, diharapkan skripsi ini bermanfaat bagi masyarakat luas dan menjadi bahan pertimbangan untuk dikembangkan.

1.4 Batasan Masalah

Untuk menghindari meluasnya materi pembahasan tugas akhir ini, maka permasalahan dibatasi hanya mencakup hal-hal berikut:

1. Penelitian dibatasi dengan menggunakan metode enkripsi RSA dan AES.
2. Aplikasi hanya dibatasi pada pembuatan pengamanan di ruang lingkup PT.XYZ
3. Aplikasi dititikberatkan pada proses pengamanan dokumen atau data berekstensi .pdf, .doc, .ppt dan .txt. Pada skripsi ini, pengamanan yang dilakukan adalah pada dokumen terkait prosedur dan metode kalibrasi.

4. Aplikasi dibuat menggunakan bahasa pemrograman HTML, CSS, dan JavaScript, serta dijalankan dengan menggunakan Web API.

1.5 Sistematika Penulisan

Dalam penulisan skripsi ini dibagi menjadi beberapa bab, yaitu:

BAB I **PENDAHULUAN**

Bab ini berisi tentang latar belakang masalah, identifikasi masalah, tujuan dan manfaat masalah, batasan masalah, dan sistematika penulisan.

BAB II **LANDASAN TEORI**

Bab ini mencakup tinjauan pustaka penelitian terdahulu yang berkaitan dengan masalah yang dibahas dan menguraikan tentang landasan teori yang berkaitan dengan judul penelitian.

BAB III **METODOLOGI PENELITIAN**

Bab ini menjelaskan secara rinci mengenai metodologi penelitian dalam merancang dan membuat aplikasi pengamanan data atau dokumen pada sebuah perusahaan dengan menggunakan algoritma kriptografi RSA.

BAB IV **PERANCANGAN SISTEM DAN PENELITIAN**

Bab ini menampilkan hasil pengujian simulasi aplikasi pengamanan data. Hasil pengujian yang ditampilkan dan dibahas merupakan hasil analisis terhadap parameter-parameter perbandingan yang ditentukan.

BAB V **PENUTUP**

Bab ini memberikan kesimpulan dan keterbatasan berdasarkan hasil yang diperoleh. Selain itu, pada bab ini juga diberikan saran-saran untuk penelitian selanjutnya berkaitan dengan pengembangan dari penelitian yang dilakukan di dalam skripsi ini.