BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi, tingkat keamanan terhadap suatu informasi yang bersifat rahasia pun semakin tinggi. Hal ini merupakan aspek yang paling penting dalam permasalahan privasi, agar informasi tidak jatuh kepada pihak yang tidak bertanggung jawab. Berbagai tindak kejahatan maupun ancaman yang merupakan masalah dari segi keamanan yang timbul dapat berupa interupsi, penyadapan, maupun modifikasi. Salah satu cara yang dapat digunakan untuk mengatasi permasalahan ini adalah dengan menggunakan teknik kriptografi. Kriptografi berperan sebagai suatu sistem pengamanan dengan menggunakan teknik enkripsi data dengan menggunakan kunci (*key*) tertentu menjadi serangkaian kode yang disebut dengan *ciphertext*.

Ide awal kriptografi adalah pemakaian algoritma yang bersifat rahasia untuk mengenkripsi data. Ini yang disebut dengan algoritma kriptografi klasik. Namun, lama-kelamaan cara ini dianggap kurang efisien dengan alasan bahwa lebih baik merahasiakan *key* untuk mengenkripsi ataupun mendekripsi data daripada merahasiakan algoritma yang digunakan. Sehingga algoritma kriptografi kunci publik mulai diperkenalkan sebagai suatu perbaikan yang masih tetap mengacu kepada kriptografi klasik.

Kebutuhan masyarakat terhadap keamanan informasi yang semakin meningkat mengakibatkan timbulnya masalah lain dalam pengaman file, yaitu salah satunya keamanan file rahasia dokumen format docx. Sehingga dalam permasalahan ini penulis tertarik melakukan penelitian untuk mengamankan data dokumen berekstensi docx. Aplikasi pengelolah kata *Microsoft Office Word* merupakan salah satu aplikasi pengolah

kata yang paling banyak digunakan khususnya di Indonesia. Penggunaan *Ms.Office Word* tidak hanya terbatas pada pengetikan untuk keperluan pribadi, tetapi juga banyak digunakan untuk keperluan perusahan yang sekaligus menjadikan *Word* sebagai salah satu elemen utama dalam pengetikan dokumen rahasia atau yang bersifat penting.

Aplikasi *Ms. Office Word* pada dasarnya telah menyediakan fasilitas proteksi berupa *password* baik untuk pengeditan ataupun pembuka file, tetapi pada saat ini telah banyak beredar secara luas utilitas untuk membuka *password* tersebut dengan mudah. Dalam permasalahan pengaman file dokumen yang bersifat rahasia atau penting, baik untuk keperluan pribadi atau keperluan perusahaan, enkripsi data yang disediakan oleh aplikasi *Ms. Office Word* tidaklah cukup, maka diperlukan suatu proteksi khusus terhadap dokumen tersebut agar tidak mudah dipecahkan oleh *Cryptanalisis,* untuk itu penulis melakukan penelitian untuk mengenkripsi dan dekripsi dokumen *Word* dengan menggunakan kombinasi metode kriptografi yaitu metode *vernam cipher* dan *hill cipher* berbasis web.

Dari hasil penelitian yang dilakukan oleh Khairani Puspita dan M. Rhifky Wayahdi tahun 2015 yang berjudul "Analisis Kombinasi Metode *Caesar Cipher, Vernam Cipher*, Dan *Hill Cipher* Dalam Proses Kriptografi" penulis dapat menyimpulkan bahwa *metode Vernam Cipher* dan metode *Hill Cipher* adalah jenis kriptografi klasik yang cukup kuat jika dilihat dari segi keamanannya, dan dari hasil analisis penelitian tersebut bahwa metode *Vernam Cipher* dan *Hill Cipher* dapat dikombinasikan menjadi satu dalam proses kriptografi (enkripsi dan dekripsi) dengan tingkat keamanan yang sangat baik dan sulit untuk dipecahkan. Pada penelitian yang dilakukan oleh Khairani Puspita dan M. Rhifky Wayahdi, kombinasi metode *Caesar Cipher, Vernam Cipher,* dan *Hill Cipher* ini hanya membutuhkan sebuah kunci (*key*) dalam proses enkripsi maupun dekripsi yang akan memudahkan kita

untuk mengingatnya. Tujuan penelitian tersebut dilakukan adalah untuk menganalisis metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dalam proses kriptografi. Penulis ingin mengkombinasikan ketiga metode tersebut dalam proses enkripsi dan dekripsi untuk meningkatkan keamanan data atau pesan.

1.2 Rumusan Masalah

Secara umum, inti dari permasalahan yang dikaji dalam penelitian ini adalah bagaimana merancang dan membangun sebuah perangkat lunak berbasis web yang dapat meningkatkan keamanan file dokumen berekstensi docx dengan mengkombinasikan metode *vernam cipher* dan *hill cipher*.

1.3 Batasan Masalah

Adapun batasan masalah yang harus diperhatikan dalam penelitian ini adalah:

1. File yang digunakan yaitu bersifat dokumen berekstensi docx.
2. File yang di enkripsi hanya file docx yang berisi teks.
3. Aplikasi yang di bangun berbasis Web.
4. Menggunakan kombinasi metode *vernam cipher* dan *hill cipher.*

1.4 Tujuan Penelitian

Adapun tujuan penelitian yaitu untuk merancang aplikasi pengaman dokumen berekstensi docx yang handal dengan kombinasi metode *vernam cipher* dan *hill cipher* agar tingkat keamanan pada dokumen semakin terjaga kerahasiaannya.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah menghasilkan suatu aplikasi berbasis web yang dapat mengenkripsi file dokumen berekstensi docx sehingga kerahasiaan file semakin terjaga dan hanya pihak yang memiliki hak atas dokumen tersebut dapat mendekripsinya.

1.6 Sistematika Penulisan

Penelitian ini terbagi ke dalam tiga bab beserta pokok materinya. Sebagai gambaran umum sistematika penyusunan proposal yang akan ditulis adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini membahas secara singkat teori yang diperlukan dalam penelitian skripsi.

BAB III METODE PENELITIAN

Pada bab ini akan disajikan metodologi yang digunakan penulis dalam melakukan penelitian.