BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan adalah suatu hal yang dituntut dalam kehidupan, dimana seluruh makhluk sangat membutuhkannya dalam memenuhi hal-hal yang berkaitan dengan maslahat kepentingan mereka, baik yang sifatnya keduniaan maupun keagamaan.

Perkembangan teknologi saat ini memungkinkan manusia untuk berkomunikasi dan saling bertukar informasi dengan jarak jauh. Pertukaran informasi jarak jauh seperti antar kota, antar wilayah dan bahkan antar benua sudah tidak menjadi kendala lagi namun dilain hal keamanan atau sekuritas terhadap kerahasiaan informasi saat inilah yang menjadi persoalan. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu.

Salah satu bentuk komunikasi data adalah dengan menggunakan tulisan teks karena banyak informasi yang dapat disampaikan melalui tulisan (teks) dan terkadang dalam teks tersebut terdapat informasi yang bersifat rahasia. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikannya. Perlindungan terhadap kerahasiaan datapun meningkat, salah satu caranya dengan penyandian data atau enkripsi.

Adapun firman Allah SWT yang berkaitan dengan keamanan yaitu QS Al-Ankabut ayat 67 yang berbunyi :

أَوَلَمْ يَرَوْا۟ أَنَّا جَعَلْنَا حَرَمًا ءَامِنًا وَيُتَخَطَّفُ ٱلنَّاسُ مِنْ حَوْلِهِمْ ۚ أَفَبِٱلْبَٰطِلِ يُؤْمِنُونَ وَبِنِعْمَةِ ٱللَّهِ يَكْفُرُونَ ﴿٦٧﴾

Artinya : Dan Apakah mereka tidak memperhatikan, bahwa Sesungguhnya Kami telah menjadikan (negeri mereka) tanah suci yang aman, sedang manusia sekitarnya rampok-merampok. Maka mengapa (sesudah nyata kebenaran) mereka masih percaya kepada yang bathil dan ingkar kepada nikmat Allah?

Kata kriptografi berasal dari bahasa Yunani yaitu krupto (*hidden* atau *secret*) dan *grafh* (*writing*) artinya "*secret writing*". Dahulu kriptografi dapat diartikan ilmu dan seni untuk menjaga keamanan data atau pesan dengan cara menyandikan ke bentuk yang tidak dapat dimengerti lagi artinya. Dalam perkembangannya, kriptografi tidak hanya diartikan untuk mengenkripsi data ataupun pesan, tetapi juga menjaga keamanan data atau pesan. Perkembangkan teknologi informasi dimasa sekarang mudah untuk melakukan komunikasi dan berbagai informasi. Tetapi dengan kemudahan itu orang lupa bahwa keamanan dan privasi data merupakan hal penting dalam komunikasi.

Enkripsi atau mengkodekan data teks dapat dilakukan dengan berbagai algoritma kriptografi, salah satunya adalah *Caesar Cipher*. Algoritma ini merupakan salah satu metode umum yang digunakan dalam kriptografi dimana digunakan pertama kali pada tahun 50 SM oleh Julius Caesar untuk mengirimkan pesan ke Marcuss Cicero. Caesar mengkodekan informasi dengan mengubah setiap huruf dalam informasi menjadi tiga huruf setelah informasi asli dalam urutan alphabet. Algoritma yang dipakai dalam *caesar chiper* sangat sederhana dan terlalu mudah untuk dipecahkan, sehingga *caesar chiper* dianggap kurang dapat menjaga kerahasiaan informasi. Proses enkripsi dan dekripsi pada algoritma *Caesar Chiper* menggunakan 26 huruf alfabet sehingga pengkodean hanya terjadi pada alfabet itu sendiri tanpa adanya spasi dan tanda baca lainnya. Enkripsi menggunakan metode *Caesar Cipher* memiliki kecepatan enkripsi yang cukup baik, ini disebabkan karena proses enkripsinya cukup sederhana dan hanya melibatkan beberapa operasi saja per-bytenya.

Algoritma *Rail Fence Cipher* (RFC) merupakan salah satu teknik kriptografi yang menggunakan pergeseran posisi dengan menggunakan kata kunci

sebagai inti dari algoritma ini dalam melakukan enkripsi dan dekripsi teks. Algoritma ini merupakan salah satu variasi implementasi *cipher* transposisi.

Pada algoritma ini plainteks dituliskan secara vertikal kebawah sepanjang n-*rails* dan menulis lagi ke kolom baru ketika telah mencapai karakter tertentu dimana *ciphertext* yang dihasilkan adalah urutan karakter yang dibaca secara horizontal (Latifah *et al*., 2017).

Algoritma *Rail Fence Cipher* (RFC) mudah untuk dibobol oleh kriptanalis dengan mencoba beberapa nilai kedalaman untuk menentukan banyaknya baris yang digunakan. Terdapat pola tertentu berdasarkan jumlah baris yang digunakan, misalnya jika ada dua baris maka huruf ke 1,3,5,... akan berada di baris pertama dan huruf ke 2,4,6,... akan ada di baris kedua (Singh *et al.*, 2012). Meskipun algoritma ini memiliki kelemahan, namun dapat dikombinasikan dengan algoritma yang lain dalam menaikkan tingkat keamanan *ciphertext*-nya sehingga tidak mudah dianalisis (Siahaan, 2016).

Algoritma Rotate13 (ROT13) merupakan pengembangan dari algoritma *Caesar cipher* dimana algoritma ini melakukan pergantian setiap karakter huruf dengan 13 karakter di depan dan satu dibelakangnya sesuai dengan alfabet dimana dilakukan pergeseran karakter ke 13 yaitu pada huruf A diganti dengan N. Agar data tersamarkan dan tidak dapat terbaca dengan sekilas maka pergeseran karakter pada tabel ASCII dengan menggeser mundur sebanyak 13 karakter (Andriyani, 2019).

Dalam penelitian ini penulis melakukan enkripsi file teks menggunakan Kombinasi algoritma *Rail Fence Cipher* (RFC) dan ROT13 (Rotate13) untuk menjaga kerahasiaan file teks. Dengan melihat latar belakang masalah diatas, maka penulis melakukan penelitian ini dengan judul **Menjaga Kerahasiaan File dengan Menggunakan Metode Rail Fence Cipher dan ROT13.**

1.2 Rumusan Masalah

Dari latar belakang sebelumnya, maka penulis merumuskan permasalahan sebagai berikut:

1. Bagaimana mengkombinasikan algoritma RFC dan ROT13 dalam mengenkripsi dan mendekripsi data agar terjaga kerahasiaannya?
2. Bagaimana menghasilkan sebuah sistem yang dapat melakukan enkripsi dan dekripsi file teks dengan mengkombinasikan algoritma RFC dan ROT13 untuk menambah tingkat keamanannya ?

1.3 Batasan Masalah

Agar pembahasan tidak menyimpang dari tujuan, maka perlu dibuat suatu batasan masalah, yaitu:

1. Aplikasi ini hanya mengenkripsi dan mendekripsi huruf alphabet (A-Z) dengan format bertipe teks (*.txt) dan word (*.doc dan *.docx).
2. Program ini mengenkripsi dan mendekripsi data menggunakan kombinasi algoritma RFC dan ROT13.
3. Program ini dirancang menggunakan bahasa pemrograman Visual Basic.NET 2010.
4. Cipherteks hasil enkripsi disimpan dalam file berformat (.hyb).

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengkombinasikan algoritma RFC dan ROT13 untuk mengenkripsi dan mendekripsi file teks.
2. Untuk menghasilkan sebuah sistem yang handal dalam melakukan enkripsi dan dekripsi data untuk meningkatkan keamanannya.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Membantu pengguna dalam mengamankan data teks agar isinya tidak dapat diketahui oleh orang yang tidak berhak.
2. Diperolehnya sebuah aplikasi keamanan data dengan menggunakan kombinasi algoritma RFC dan ROT13.