BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi sekarang ini mengalami peningkatan yang sangat signifikan bagi kehidupan manusia. Perkembangan teknologi informasi memudahkan pengguna untuk menyelesaikan setiap aktifitas dengan cara-cara yang lebih praktis, seperti kegiatan dalam melakukan komunikasi antar satu dengan yang dibatasi oleh jarak dan juga berupa aktifitas untuk mengetahui informasi penting secara real time. Pesatnya perkembangan teknologi informasi diberbagai bidang tak terlepas dari manfaatnya untuk membuat, menyimpan dan menyebarkan informasi. Manfaat teknologi informasi tidak hanya penting dalam dunia telekomunikasi namun bisa dirasakan dari berbagai bidang seperti bidang kesehatan, bidang bisnis, bidang pendidikan dan bidang perbankan.

Penggunaan teknologi informasi memiliki dampak yang positif dan juga negatif bagi manusia, tergantung cara individu dalam memanfaatkan teknologi yang ada. Sisi positif yaitu kemudahan mengakses informasi, memudahkan dalam komunikasi, memperbanyak relasi melalui media sosial dan mampu membantu menyelesaikan permasalahan dengan mudah. Namun penggunaan teknologi informasi yang semakin canggih memiliki dampak negatif seperti bagi kehidupan manusia diantaranya; konten negative sangat mudah diakses serta bisa diakses oleh siapapun dan dimanapun, malas bersosialisasi secara fisik, meningkatkanya penipuan dan munculnya kejahatan *cyber*.

Kemudahan dalam pertukaran informasi dalam sebuah jaringan internet memunculkan berbagai ancaman kejahatan atau *cyber crime* yang membuat informasi bisa diambil dan dimodifikasi tanpa persetujuan dari pihak yang bersangkutan. Ancaman *cyber crime* merupakan sebuah kondisi dan situasi yang dapat dinilai melakukan serangan yang mampu merusak dan merugikan serta mengancam kerahasiaan, integritas dan ketersediaan sistem dan informasi (Rahmawati 2017). Dengan munculnya ancaman kejahatan ini menyebabkan para pengguna internet dalam melakukan komunikasi menjadi lebih waspada untuk mengirimkan informasi yang bersifat rahasia dengan yang lain. Akan tetapi, kebutuhan akan komunikasi memaksa pengguna internet untuk terus menggunakan fasilitas yang ada sehingga memunculkan ide-ide untuk mengamankan pesan agar kerahasiaan pesan yang ingin disampaikan bisa terjaga dan bisa terkirim kepenerima tanpa adanya perubahan isi pesan. Serangan-serangan yang bisa dilakukan dalam pengiriman pesan bisa berupa *interception* yaitu serangan yang ditujukan pada aspek privasi yang mana pihak yang tidak berwenang dapat mengakses informasi dan serangan lain berupa *modification* yaitu serangan di bertujuan untuk memodifikasi isi pesan (Novenzo Ihsana and Maslan 2020).

Kerahasiaan dan keamanan suatu informasi yang akan dikirim sehingga bisa sampai kepenerima yang telah ditentukan merupakan aspek yang sangat penting. Untuk mendukung keamanan data dan kerahasiaanya digunakan teknik kriptografi. Teknik ini dilakukan agar pesan yang akan di kirim tidak diketahui oleh orang lain dan hanya bisa diakses oleh pengguna yang telah ditentukan. Kriptografi adalah ilmu dan seni untuk

menjaga pesan dengan cara menyandikan kedalam bentuk yang tidak dapat dimengerti lagi maknanya (Munir 2019).

Teknik kriptografi yang diaplikasikan dalam keamanan pesan atau informasi pada pembahasan ini adalah menggunakan algoritma *caesar cipher*. *Caesar cipher* adalah teknik enkripsi di mana setiap karakter dalam pesan terenkripsi diganti sebagai kunci dengan menggeser urutannya. Misalnya, setiap huruf diganti dengan huruf ketiga yang paling dekat dengan alfabet. Tujuan kriptografi untuk mendapatkan keutuhan, kerahasiaan dan keaslian dari sumber informasi yang telah disampaikan oleh pengirim pesan. Pada kriptografi dikenal beberapa istilah antara lain kode disebut *ciphers*, pesan yang disembunyikan disebut plain text, pesan yang akan diubah bentuk sehingga orang lain tidak mengerti maknanya disebut *ciphertext*. Proses yang dilakukan dalam mengubah isi dari pesan disebut enkripsi, sementara untuk mengembalikan makna dari pesan yang diterima disebut deskripsi. Untuk menjamin kerahasian dan keutuhan dari pesan yang akan disampaikan maka penulis tertarik untuk mengangkat pembahasan dengan judul "**Implementasi *caesar cipher* pada algoritma kriptografi klasik dalam penyandian pesan**"

1.2 Identifikasi Masalah

Pada penelitian ini, penulis akan mengidentifikasi permasalahan yang menjadi masalah utama yaitu:

1. Isi pesan yang hendak disampaikan bisa disalahgunakan.
2. Bisa diketahui isi pesan oleh pihak yang tidak berkepentingan

3. Isi pesan bisa dimodifikasi sehingga berbeda dengan tujuan pesan yang sesungguhnya.

1.3 Batasan Masalah

Berdasarkan latar belakang diatas, maka perlu dibatasi pembahasan pada skripsi antara lain:

1. Melakukan enkripsi dan deskripsi pada pesan yang berisikan huruf
2. Melakukan enkripsi dan deskripsi menggunakan algoritma *caesar cipher.*

1.4 Rumusan Masalah

Bagaimana cara mengimplementasikan pengamanan pesan menggunakan algoritma *caesar cipher*

1.5 Tujuan Penelitian

Untuk merancang sistem pengamanan pada proses pengiriman pesan menggunakan algoritma *caesar cipher*

1.6 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah:

1. Meningkatkan pengetahuan tentang proses penyandian teks menggunakan *caesar cipher*
2. Meningkatkan pengetahuan dalam mengembalikan isi pesan yang telah disandikan.
3. Dapat menjadi bahan referensi dalam menambah pengetahuan untuk melakukan penelitian pada masa selanjutnya.