# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Pada masa sekarang ini industri sudah mencapai versi 4.0 dimana hampir semua pekerjaan yang dulunya dikerjakan secara manual oleh manusia sekarang sudah terkomputerisasi dan otomatis. Tak dapat dihindari lagi tren, pekerjaan, bisnis dan bahkan gaya hidup umat manusia sedikit demi sedikit berganti menyesuaikan dengan perkembangan teknologi yang sedang terjadi.

Perkembangan ini memuncukan tahapan baru yang di alami umat manusia yaitu masyarakat informasi, masyarakat yang melakukan kegiatan distribusi, penggunaan dan manipulasi informasi dalam aktivitas ekonomi, politik, sampai budaya secara signifikan. Hal ini membuat keamanan dan kerahasiaan informasi menjadi hal yang sangat penting dan perlu mendapat perhatian lebih. Dari hal ini juga segala informasi yang ada membutuhkan standar keamanan demi menjaga ke-absahan, validitas dan kerahasiaan dalam pertukarannya.

Adapun bahaya yang biasanya mengancam dalam pertukaran informasi adalah penyadapan. Hal ini biasa dilakukan oleh oknum yang tidak bertanggung jawab melalui suatu jaringan internet, apalagi jika pertukarannya dilakukan melalui jaringan publik, apabila data tidak diamankan terlebih dahulu akan sangat rentan disadap dan diketahui isi dari informasi tersebut mengingat informasi yang dibagikan hanya dapat dilihat oleh pihak – pihak tertentu saja.

Salah satu cara yang digunakan dalam pengamanan informasi adalah dengan menggunakan kriptografi, yaitu sebuah ilmu yang membahas tentang bagaimana cara merahasiakan suatu informasi. Jadi dengan kriptografi kita dapat dengan aman dalam bertukar informasi. Dengan kriptografi walaupun informasi yang dibagikan atau didapatkan jatuh ke tangan penyadap, data tidak bisa diketahuhi oleh pelaku.

Dalam perkembengannya kriptografi mengalami banyak kemajuan, penelitian tentang kriptografi sudah banyak dilakukan namun tidak sedikit juga orang yang mempunyai niat jahat mengetahui algoritma – algoritma kriptografi sehingga dapat

mengetahui isi informasi walaupun sudah diamanakan. Oleh karena itu penelitian tentang kriptografi akan selalu berkembang untuk memperoleh algoritma kriptografi yang semakin kuat.

Penelitian ini akan mencoba mengembangkan salah satu metode dalam kriptografi yaitu *Caesar Cipher*, sebuah metode lama yang dikembangkan oleh Julius Caesar. Metode ini sangat mudah dipecahkan oleh karena itu penulis ingin mengembangkan sebuah metode yang menggabungkan antara metode *Caesar Cipher* dengan metode enkripsi matriks dan algoritma *Fisher Yates Shuffle* untuk pengacakan urutan abjad yang akan digunakan untuk melakukan enkripsi.

## 1.2 Perumusan Masalah

Rumusan masalah yang dapat didefinisikan pada penelitian ini adalah sebagai berikut:

1. Bagaimana mengembangkan metode kriptografi *Caesar chipper*?
2. Bagaimana mengimplementasikan algoritma yang sudah dikembangkan ke dalam aplikasi *chatting* sederhana?

## 1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengembangkan metode kriptografi *Caesar chipper* dan matrix dengan pengacakan abjad menggunakan algoritma *fisher yates shuffle* dan algoritma *Diffie-Hellman* sebagai metode pertukaran kuncinya.
2. Mengimplementasikan metode kriptografi yang dikembangakan ke dalam aplikasi *chatting* sederhana.

## 1.4 Manfaat Penelitian

Manfaat penelitian ini secara umum dapat menghasilkan metode kembangan baru kombinasi dari metode *caesar cipher* dan matrix yang dalam pengacakan abjadnya menggunakan algoritma *fisher yates shuffle* dan *diffie-hellman* sebagai metode pertukaran kunci pergeserannya sehingga dapat diimplementasikan dalam suatu aplikasi sebagai salah satu pengaman dalam pertukaran informasi yang berbentuk text.

Adapun manfaat penelitian untuk dunia akademik adalah sebagai berikut:

1. Dapat menjadi referensi untuk penelitian selanjutnya
2. Dapat menjadi bahan belajar
3. Penelitian ini dapat dikembangkan secara lanjut

Adapun manfaat penelitian ini untuk penulis sendiri adalah:

1. Menambah pengetahuan dalam dunia kriptografi
2. Menjadi jembatan untuk memperluas pengetahuan bukan hanya di dunia kriptografi juga dalam dunia pengetahuan teknologi informasi pada umumnya.
3. Dapat menjadi syarat lulus kuliah strata satu

## 1.5 Batasan Masalah

Agar pembahasan tidak melebar dan tidak seuai dengan apa yang akan dikerjakan dalam penelitian ini, maka penulis memberikan batasan – batasan masalah sebagai berikut:

1. Penelitian hanya berfokus pada pengembangan algoritma *caesar cipher* dan pengembangan aplikasi *chatting* sederhana.
2. Aplikasi *chatting* sederhana hanya untuk mencoba mengimplementasikan algoritma *caesar cipher* yang dikembangkan.
3. Pegimplementasian algoritma yang dikembangkan bertujuan untuk mengamankan pesan pada saat pengiriman ke sisi *server* maupun ke sisi *client*.