**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Matematika sebagai ilmu pengetahuan dasar sangat berpengaruh penting dalam perkembangan ilmu pengetahuan lainnya, termasuk perkembangan teknologi informasi. Perkembangan teknologi informasi mempunyai pengaruh yang sangat signifikan bagi aspek kehidupan, tidak terkecuali aspek komunikasi dan pengiriman pesan maupun pengiriman data. Masalah keamanan dan kerahasiaan data merupakan hal yang penting . Data yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai *file* di dalam komputer maupun saat data tersebut dikirim melalui *e-mail*.

Untuk menyimpan data tersebut agar benar-benar aman, tentunya dilakukan sistem pengamanan yang baik, yang bebas dari jangkauan orang-orang yang tidak berhak, baik bebas dari jangkauan secara fisik maupun secara sistem. Untuk bebas secara fisik, maka faktor orang sebagai penjaga memegang peranan yag penting, sedangkan aman menurut sistem adalah dokumen tersebut tersimpan dalam kondisi yang tidak dapat dibaca oleh orang lain yang tidak berhak. Apalagi jika data tersebut berada dalam suatu jaringan komputer yang terhubung ataau terkoneksi dengan jaringan internet. Tentu saja data tersebut tidak boleh diketahui apalagi diubah oleh pihak yang tidak berwenang.

Suatu pesan rahasia dapat diterapkan pada ilmu kriptografi yang merupakan suatu ilmu seni dengan filosofinya the art of war, dimana waktu tersebut pernah digunakan untuk mengirim pesan rahasia pada jaman romawi pada era raja Julius Caesar. Tujuannya agar pembajak surat rahasia tidak dapat membaca pesannya secara langsung oleh orang lain jika belum di deskripsikan dengan metode tertentu.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim, di sandikan bentuknya dalam kode-kode tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi asli. Ada beberapa contoh macam-macam metode kriptografi untuk membuat pesan rahasia antara lain : *Caesar*, *Affine*, *monoalphabetic, Polyalphabetic, Vigenere, Beaufort, Playfair,* Transposisi, MD5, DES, RSA, DSA, ElGamal, dan SHA.

Algoritma kriptografi dibagi menjadi dua bagian berdasarkan kunci yang dipakainya yaitu Algoritma Kriptografi Kunci Simetris (*symmetric-key cryptography algorithm)* dan Algoritma Kriptografi Simetris (a*symmetric-key cryptography algorithm).*

Algoritma kriptografi kunci asimetris biasa disebut algoritma kriptografi kunci publik (*public key cryptography algorithm*). Jenis ini menggunakan kata kunci untuk melakukan enkripsi dan dekripsi yang berbeda, yaitu kunci publik yang digunakan untuk proses enkripsi pesan yang sifatnya boleh diketahui semua orang (dipublikasikan) serta kunci privat yang digunakan untuk proses dekripsi yang sifatnya rahasia dan hanya diketahui oleh penerima pesan yang bersangkutan. Jenis kriptografi kunci publik diantaranya adalah RSA (*Rivest, Shamir,Adleman*), ElGamal dan algoritma kriptografi berbasis kurva Eliptik.

Algoritma kriptografi kunci simetris biasa disebut algoritma kriptografi kunci rahasia (*private key cryptography algorithm*) atau algoritma kriptografi klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm* . Jenis jenis kriptografi simetris di antaranya adalah DES, IDEA, AES, *Vigenere,* A5, OTP, *Blowfish,Twofish* dan sejenisnya.

*Vigenere* merupakan salah satu kriptografi kunci simetris yang pertama kali dipopulerkan oleh *Blaise de Vigenere* seorang diplomat prancis pada abad ke-15, sehingga disebutlah metode ini denga sistem sandi *Vigenere*. Sistem sandi *Vigenere* adalah sistem sandi substitusi multi-alfabet, yaitu sistem sandi Caesar tetapi dengan pergeseran alphabet yang berlainan disesuaikan dengan kata kunci. Yang dimaksud sistem sandi substitusi adalah menyandi dengan cara mengganti huruf-huruf pesan/teks aslinya dengan huruf-huruf sandi. Sistem sandi Caesar dan *Vigenere* termasuk metode sistem sandi ini. bahkan sistem sandi substitusi merupakan sistem sandi yang dipakai pula dalam kriptografi modern, dengan variasi-variasi yang terus berkembang.

Sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Pada saat kejayaannya, sandi ini dijuluki *le chiffre indechiffrable* (Sandi yang tak terpecahkan). Metode pemecahan sandi ini baru ditemukan pada abad ke-19. Pada tahun 1854, *Charles Babbage* menemukan cara untuk memecahkan sandi *Vigenere*. Metode ini dinamakan *tes kasiski* karena *Frierich Kasiski-*lah yang pertama mempublikasikannya.

Penerapan metode *Vigenere* kriptografi untuk membuat aplikasi kriptosistem di Microsoft Visual Studio dalam suatu text rahasia yang dibutuhkan agar setiap pesan yang kita miliki tidak dapat dibaca oleh pembajak. Pengembangan sistem menggunakan metode *vigenere* dapat membuat suatu pesan rahasia tidak mudah dibaca langsung oleh orang lain. Pengirim (*sender*) pesan text asli (*plaintext*) berupa suatu kalimat yang di enkripsi oleh kriptosistem untuk mengacak pesan aslinya dengan menggunakan kunci (*key*) menjadi *Ciphertext* dan dapat dikembalikan kepesan aslinya atau didekripsikan. Tujuan penerapan kriptografi adalah untuk membuat sesuatu yang tersembunyi, dapat suatu pesan rahasia berupa text, suara, gambar dan video.

Penelitian mengenai Kriptografi *Vigenere* pun telah banyak dilakukan oleh para kriptonalisis, antara lain hijasma mushlih (2012) Pembuatan aplikasi kriptosistem menggunakan metode algoritma *vigenere cipher*. Wiwiek Nurwiyati dan Indra Yatini B (2013) Enkripsi Dekripsi data menggunakan metode stream dan vigenere cipher. Kevin Chandra Irwanto (2013) Aplikasi teori bilangan dalam sandi vigenere dan Caesar.. Beberapa penelitian terdahulu di atas terlihat bahwa kebanyakan menggabungkan metode vigenere dengan metode lain.

Oleh karena itu, pada penelitian ini dibahas tentang bagaimana cara untuk mengenkripsikan dan mendekripsikan data dengan metode vigenere tanpa gabungan dari metode lain.

Berdasarkan uraian diatas, penulis tertarik untuk mengkaji lebih lanjut dengan mengangkat judul ***“Kriptografi Menggunakan Metode Vigenere untuk Text Message”.***

1. **Rumusan Masalah**

Berdasarkan latar belakang yang dikemukakan sebelumnya, maka rumusan masalah pada penelitian ini adalah :

1. Bagaimana konsep matematis, yang melandasi terbentuknya algoritma Kriptografi *Vigenere*?
2. Bagaimana proses enkripsi dan dekripsi menggunakan algoritma kriptografi *Vigenere* untuk *Text Message*?
3. Bagaimana mengimplementasikan algoritma kriptografi *Vigenere* pada bahasa pemrograman *Microsoft Visual Studio*?
4. **Batasan Masalah**

Penelitian ini difokuskan pada konsep matematis, proses enkripsi, dekripsi, serta proses kriptografi untuk *text message* menggunakan metode *vigenere*.

1. **Tujuan Penelitian**

Penelitian ini bertujuan untuk menjawab masalah-masalah yang telah dirumuskan. Adapun tujuan penelitian ini dapat mengetahui :

1. Konsep matematis, yang melandasi terbentuknya algoritma kriptografi *Vigenere*.
2. Proses enkripsi dan dekripsi menggunakan algoritma kriptografi *Vigenere* untuk *Text Message.*
3. Mengimplementasikan algoritma kriptografi *Vigenere* pada bahasa pemrograman *Microsoft Visual Studio*.
4. **Manfaat Penelitian**

Adapun manfaat yang diperoleh dari penelitian ini adalah :

1. Manfaat bagi penulis

Menambah pengetahuan dan wawasan, serta bahan dalam penerapan dalam matematika, khususnya pada algoritma kriptografi *Vigenere.*

1. Manfaat bagi Universitas Negeri Makassar

Dalam rangka pengembangan ilmu pengetahuan dan teknologi untuk penelitian serta sebagai rujukan referensi sehingga nantinya bisa diadakannya penelitian yang lebih mendalam tentang hal ini.

1. Manfaat bagi pihak lain yang terkait

Sebagai bahan perbandingan bagi penulis-penulis lain dibidang yang sama serta dapat memberikan informasi yang berguna untuk penelitian selanjutnya.