

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan informasi yang pesat telah membawa banyak manfaat bagi peradaban manusia, namun juga menimbulkan tantangan serius terhadap keamanan data. Ancaman terhadap data pribadi semakin meningkat seiring dengan kemajuan teknologi, sehingga perlindungan data menjadi sangat penting. Salah satu metode yang digunakan untuk mengamankan data adalah kriptografi.

Kriptografi merupakan bidang yang penting dalam menjaga keamanan informasi, dan pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah mengubah data asli (*plaintext*) menjadi data rahasia (*ciphertext*) yang dikirimkan melalui media komunikasi. Pada saat *ciphertext* diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan asli melalui proses dekripsi, sehingga pesan tersebut dapat dibaca kembali oleh penerima pesan. Dengan demikian, enkripsi dilakukan pada saat pengiriman untuk mencegah akses tidak sah pada informasi yang dikirimkan, sedangkan dekripsi dilakukan pada saat penerimaan untuk memulihkan data asli [1].

Super enkripsi merupakan penggabungan beberapa metode kriptografi

untuk meningkatkan keamanan data. Penggabungan beberapa metode ini mengakibatkan lebih banyak waktu untuk proses enkripsi. Meskipun demikian, hal ini memberikan peningkatan keamanan [2]. Pada tahun 2019, Megan-tara dkk. [3] melakukan super enkripsi dengan menggunakan algoritma Hill *cipher* pada proses enkripsi pertama dan metode transposisi kolom digunakan pada proses enkripsi kedua. Kemudian pada tahun 2023, Agustina dkk. [2] melakukan super enkripsi dengan menggunakan menggunakan algoritma Vigenere *cipher* untuk proses enkripsi yang pertama dan menggunakan algoritma *bifid cipher* untuk proses enkripsi yang kedua.

Berdasarkan pada peneltian sebelumnya, pada penelitian ini akan dikaji super enkripsi dengan menggunakan algoritma Vigenere *cipher* sebagai proses enkripsi pertama kemudian menggunakan modifikasi Hill *cipher* sebagai proses enkripsi kedua dan invers kiri matriks sebagai proses dekripsi. Pada algoritma Hill *cipher*, kunci yang digunakan berupa matriks bujur sangkar, yang telah menjadi praktik umum. Namun, pendekatan ini rentan terhadap prediksi dan serangan, karena bentuk matriks yang sederhana dan mudah diketahui. Untuk meningkatkan keamanan, modifikasi Hill *cipher* mengusulkan penggunaan matriks persegi panjang sebagai kunci. Penggunaan matriks persegi panjang ini diharapkan dapat mengatasi kelemahan yang ada pada algoritma asli, menjadikannya lebih sulit diketahui dan lebih aman.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang dibahas pada tugas akhir ini adalah bagaimana super enkripsi menggunakan algoritma Vigenere *cipher* dan modifikasi Hill *cipher* menggunakan invers kiri matriks.

1.3 Tujuan Penelitian

Berdasarkan permasalahan di atas, maka tujuan dari penelitian tugas akhir ini adalah melakukan super enkripsi menggunakan algoritma Vigenere *cipher* dan modifikasi Hill *cipher* menggunakan invers kiri matriks.

1.4 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terdiri dari empat bab. Bab I Pendahuluan yang memuat latar belakang, perumusan masalah, tujuan penulisan dan sistematika penulisan. Bab II Landasan teori yang berisi tentang materi dasar dan materi pendukung yang akan digunakan untuk menyelesaikan permasalahan pada tugas akhir ini. Bab III Pembahasan yang berisi tentang super enkripsi dengan algoritma Vigenere *cipher* dan modifikasi Hill *cipher* dengan invers kiri matriks. Bab IV Penutup yang di dalamnya berisi kesimpulan dari penulisan tugas akhir ini.