BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Zaman yang berkembang menyebabkan adanya dampak pada kemajuan teknologi. Mayoritas dari lapisan masyarakat kini memanfaatkan teknologi dalam kehidupan sehari-hari, ditambah adanya kemudahan dalam mengakses internet dimanfaatkan sebagai sarana komunikasi dan bertukar informasi. Namun, dalam pengiriman data tersebut tidak ada jaminan keamanandari pihak ketiga yang bisa saja mengaksesnya secara diam-diam.

Untuk menjaga integritas data, maka sangat diperlukan keamanan data agar data yang dikirim tidak dapat diketahui oleh pihak ketiga atau sering disebut dengan *hacker*. Terdapat salah satu metode yang bisa digunakan untuk mengamankan data dan informasi dengan teknik kriptografi.

Kriptografi merupakan suatu ilmu atau metode untuk mengamankan pesan (*message*) sehingga data yang dikirim hanya dapat diakses oleh pengirim dan penerima saja. Langkah-langkah dalam kriptografi disebut dengan algortima kriptografi. Pada pengaplikasiannya, data akan ditransmisikan dalam bentuk *ciphertext* dan ciphertext dikembalikan menjadi *plaintext* pada penerima [1].

Algoritma kriptografi memiliki banyak jenis, salah satunya adalah *Hill Cipher*. *Hill Cipher* merupakan algoritma kriptografi dengan kunci simetris yaitu hanya menggunakan satu kunci dalam proses enkripsi dan dekripsinya. Algoritma *Hill Cipher* menggunakan sebuah matriks nonsingular (memiliki *invers*) sebagai matriks kunci dan sebagai patokan ukuran blok dalam pengelompokan pesan (*plaintext*) ketika proses enkripsi dan dekripsi [2].

Algoritma *Hill Cipher* memberikan keamanan yang lebih kuat dan sulit dipecahkan jika hanya diketahui *ciphertext*nya, karena dibutuhkan matriks dan inversnya. Dibalik kelebihan yang dimiliki algoritma *Hill Cipher*, sebenarnya algoritma ini tetap memiliki celah untuk diserang oleh pihak ketiga terutama bagi orang yang mengerti tekniknya sehingga tingkat keamanannya menjadi menurun. Selain itu, penggunaan kunci simetris menyebabkan adanya kelemahan yaitu

harus dikirim melalui jalur yang aman agar pihak ketiga tidak dapat mengetahuinya [3].

Oleh karena itu, adanya modifikasi pada algoritma *Hill Cipher* ini akan membantu meningkatkan keamanan data. Modifikasi yang dapat dilakukan adalah dengan menggunakan algoritma *Huffman*, dan *Rectangular Matrix* atau Matriks Persegi Panjang.

Algoritma *Huffman* banyak digunakan dalam kompresi teks. Tujuan dari algoritma *Huffman* adalah untuk mengompres teks atau data agar ukuran file menjadi lebih kecil dari ukuran file aslinya dengan merubah susunan data menjadi data yang baru dan telah tersandikan, juga dapat mengembalikan data ke bentuk awal [3].

Matriks persegi panjang adalah matriks yang susunan bilangannya membentuk persegi panjang yang disusun menjadi kolom dan baris. Matriks ini nantinya akan digunakan sebagai matriks kunci pada algoritma *Hill Cipher* dengan catatan harus mempunyai *pseudo-inverse* atau invers semu. Penggunaan matriks persegi panjang lebih aman dibanding matriks persegi karena menghasilkan ukuran *ciphertext* yang berbeda dengan *plaintext*nya [6].

Berdasarkan uraian ini, maka penulis tertarik untuk melakukan penelitian dalam memodifikasi algoritma *Huffman* dengan algoritma *Hill Cipher* yang mana matriks kuncinya menggunakan matriks persegi panjang. Dengan demikian, penelitian skripsi ini berjudul "Teknik Enkripsi Pesan Teks Menggunakan Modifikasi *Huffman* dan *Hill Cipher* dengan Kunci Matriks Persegi Panjang".

1.2 Rumusan Masalah

Berdasarkan latar belakang sebelumnya, penulis merumuskan masalah pada penelitian kali ini yaitu :

1. Bagaimana proses pengkodean teks menggunakan algoritma *Huffman* yang dimodifikasi dengan XOR dan Teorema *Euclidean*?
2. Bagaimana pembentukan matriks kunci persegi panjang beserta inversnya?

3. Bagaimana proses modifikasi algoritma *Hill Cipher* menggunakan kunci matriks persegi panjang?
4. Bagaimana penerapan algoritma *Huffman* yang sudah dimodifikasi dengan algoritma *Hill Cipher* untuk pengiriman pesan teks?

1.3 Batasan Masalah

Agar hasil yang diperoleh sesuai dengan rumusan masalah, penulis membatasi kajian penelitian agar tidak keluar dari tujuan yang diharapkan, antara lain:

1. Algoritma pengkodean pesan yang dikaji yaitu algoritma *Huffman* dan algoritma *Hill Cipher*.
2. Data atau informasi yang akan dikodekan adalah pesan teks yang tersusun dari karakter ASCII *printable characters* yaitu karakter dengan rentang nilai 32 sampai 126.
3. Matriks yang digunakan sebagai matriks kunci untuk proses enkripsi dan dekripsi pada algoritma *Hill Cipher* adalah matriks persegi panjang dengan *full column rank*.

1.4 Tujuan Penelitian

Pada penelitian skripsi ini, beberapa tujuan yang ingin penulis capai, diantaranya sebagai berikut :

1. Menjelaskan proses modifikasi algoritma *Huffman* dengan XOR dan Teorema *Euclidean*.
2. Menjelaskan proses pembentukan matriks kunci persegi panjang beserta inversnya.
3. Membuktikan dan menjelaskan proses modifikasi algoritma *Hill Cipher* menggunakan matriks persegi panjang sebagai matriks kunci.
4. Menjabarkan tahapan simulasi pengiriman pesan teks pada algoritma *Huffman* yang sudah dimodifikasi dengan algoritma *Hill Cipher*.

1.5 Metode Penelitian

Metode penelitian yang penulis gunakan dalam penyusunan skripsi ini yaitu:

1. Pendekatan teoritis dari berbagai sumber seperti buku, jurnal, tesis, skripsi, hingga artikel di website untuk menunjang penelitian.
2. Proses studi literatur yaitu mengumpulkan, memahami, serta mengkaji teori dan berbagai informasi mengenai algoritma *Hill Cipher.*
3. Implementasi atau pengaplikasian hasil modifikasi algoritma *Huffman* dan *Hill Cipher* dengan menggunakan data pesan teks.

1.6 Sistematika Penulisan

Sistematika penulisan yang penulis gunakan dalam skripsi ini terbagi menjadi beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian serta sistematika penulisan skripsi.

BAB II LANDASAN TEORI

Bab ini berisi tentang dasar-dasar teori yang bersesuaian dengan permasalahan yang dikaji pada skripsi ini. Secara umum teori yang dipaparkan mencakup Algoritma *Huffman* secara umum, Operasi XOR, Teorema *Euclidean*, Operasi Matriks, Kriptografi secara umum, dan Algoritma *Hill Cipher*.

BAB III TEKNIK ENKRIPSI PESAN TEKS MENGGUNAKAN MODIFIKASI HUFFMAN DAN HILL CIPHER DENGAN KUNCI MATRIKS PERSEGI PANJANG

Bab ini berisi inti pembahasan dari permasalahan yang di kaji dalam skripsi. Pembahasan tersebut adalah menjelaskan proses pengiriman pesan teks menggunakan Algoritma *Huffman* yang dimodifikasi dengan proses XOR dan Teorema *Euclidean*, kemudian menggunakan Algoritma *Hill*

Cipher dengan matriks kunci berupa matriks persegi panjang.

BAB IV PENUTUP

Bab ini merupakan bagian akhir dari penulisan yang berisi kesimpulan atas semua pembahasan serta saran untuk pengembangan topik pembahasan skripsi.