BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era teknologi saat ini, keamanan data menjadi salah satu aspek terpenting dalam pengembangan sistem informasi, khususnya dalam sistem e-commerce yang menyimpan berbagai data penting seperti identitas pengguna. Tanpa adanya perlindungan yang memadai, data tersebut sangat rentan terhadap berbagai jenis serangan siber, seperti penyadapan, pencurian data, dan akses ilegal oleh pihak yang tidak berwenang [2].

Salah satu pendekatan yang umum digunakan untuk melindungi data adalah *kriptografi*, yaitu metode untuk mengubah data asli (*plaintext*) menjadi bentuk terenkripsi (*ciphertext*) yang tidak dapat dibaca tanpa kunci tertentu. Dengan cara ini, meskipun data berhasil diakses oleh pihak ketiga, isinya tetap tidak dapat dimengerti tanpa proses *dekripsi* yang tepat [3].

Secara umum, *kriptografi* terbagi menjadi dua jenis: *kriptografi* klasik dan *kriptografi* modern. Meskipun dianggap sederhana dan telah lama digunakan, *kriptografi* klasik tetap relevan dalam berbagai konteks, terutama dalam bidang pendidikan, penelitian, dan sistem berskala kecil karena kemudahannya dalam implementasi [2].

Dua algoritma *kriptografi* klasik yang umum digunakan adalah *Hill Cipher* dan *Affine Cipher*. *Hill Cipher* memanfaatkan prinsip *matriks* dan operasi matematika untuk mengkonversi blok huruf menjadi format kode. Dengan memanfaatkan blok dan *matriks* sebagai kunci, algoritma ini menciptakan *ciphertext* yang lebih rumit dan lebih sulit untuk dikenali [3]. Sementara itu, *Affine Cipher* adalah algoritma yang meggunakan rumus linier dasar dengan dua bilangan sebagai kunci, yaitu angka untuk mengalikan dan angka untuk menambah.

Beberapa penelitian sebelumnya telah menganalisis algoritma ini dari sudut pandang yang berbeda. Penelitian oleh Adnan Buyung Nasution (2020) memodifikasi *Affine Cipher* dengan menambahkan proses membalik karakter

sebelum tahap enkripsi. Hasilnya menunjukkan bahwa tingkat keacakan *ciphertext bertambah*, meskipun belum diuji untuk serangan keamanan secara langsung [5]. Nurharianna Siregar dkk (2022) menggunakan *Hill Cipher* untuk mengenkripsi file teks ASCII dengan matriks 2×2. Dengan demikian, algoritma ini mampu menyimpan pesan secara efisien dalam file teks [6]. Penelitian oleh Roman Gusmana, dkk (2023) menciptakan simulasi aplikasi enkripsi dengan *Hill Cipher* dan menemukan bahwa bentuk sandi yang dihasilkan cukup rumit dan sulit untuk ditebak [7]. Putra, dkk (2024) menganalisis perbandingan antara *Hill Cipher* dan *Affine Cipher* dalam konteks perlindungan data citra digital. Hasilnya, Hill Cipher mencatat nilai MSE sebesar 7073,40 dan PSNR sebesar 9,63 dB, yang menunjukkan bahwa *Hill Cipher* lebih efektif dalam menyembunyikan data visual [8].

Untuk menguji cara kerja kedua algoritma ini dalam melindungi keamanan data, diperlukan perbandingan secara langsung dalam sistem yang mirip dengan kondisi sebenarnya. Dalam penelitian ini, sistem e-commerce berbasis web digunakan sebagai alat simulasi untuk menerapkan algoritma *Hill Cipher* dan *Affine Cipher*. Melalui uji ini, kedua algoritma akan dianalisis dari segi proses enkripsi, dekripsi, serta ketahanan keamanan ciphertext terhadap pendekatan *Ciphertext-Only Attack* (COA) dan pengukuran tingkat keacakan menggunakan *Shannon Entropy*.

1.2 Rumusan Masalah

Dalam konteks ini, permasalahan yang dihadapi adalah keamanan data pada web e-commerce yang menyimpan informasi sensitif seperti data pengguna. Untuk mengatasi hal tersebut, algoritma kriptografi klasik seperti *Hill Cipher* dan *Affine Cipher* dapat diterapkan sebagai upaya menjaga kerahasiaan data. Namun, kedua algoritma tersebut memiliki pendekatan dan tingkat kompleksitas yang berbeda, sehingga efektivitasnya dalam menjaga keamanan belum dapat disimpulkan secara pasti. Sementara itu, masih minim penelitian yang membandingkan keduanya secara langsung dalam skenario sistem web yang nyata. Oleh karena itu, diperlukan perbandingan guna mengetahui algoritma mana yang lebih unggul serta sejauh mana masing-masing mampu melindungi data berdasarkan analisis keamanan

ciphertext melalui pendekatan *Ciphertext-Only Attack* (COA) dan pengukuran tingkat keacakan menggunakan *Shannon Entropy*.

1.3 Batasan Masalah

Agar pembahasan dalam penelitian ini lebih terarah dan tidak menyimpang dari permasalahan yang telah dirumuskan, maka ruang lingkup penelitian dibatasi sebagai berikut:

1. Penelitian ini difokuskan pada pengamanan data pengguna pada sistem e-commerce berbasis web sebagai media simulasi pengujian.
2. Algoritma kriptografi yang digunakan dalam penelitian ini dibatasi pada algoritma kriptografi klasik, yaitu *Hill Cipher* dan *Affine Cipher*.
3. Data yang diamankan dalam penelitian ini hanya berupa data teks pengguna, yang meliputi username, email, dan password.
4. Pengujian performa pada penelitian ini dibatasi pada pengukuran waktu proses enkripsi dan dekripsi.
5. Analisis keamanan difokuskan pada ciphertext yang dihasilkan oleh masing-masing algoritma, dengan pendekatan *Ciphertext-Only Attack* (COA).
6. Pengukuran tingkat keacakan ciphertext dilakukan menggunakan metode *Shannon Entropy*.

1.4 Tujuan

Tujuan penelitian ini adalah sebagai berikut:

1. Menjelaskan cara kerja algoritma *Hill Cipher* dan *Affine Cipher* sebagai bagian dari kriptografi klasik.
2. Menerapkan kedua algoritma tersebut dalam sistem web e-commerce untuk proses enkripsi dan dekripsi data.
3. Membandingkan tingkat keamanan algoritma *Hill Cipher* dan *Affine Cipher* berdasarkan analisis keamanan ciphertext menggunakan pendekatan *Ciphertext-Only Attack* (COA) dan pengukuran tingkat keacakan dengan *Shannon Entropy*.

1.5 Manfaat

Penelitian ini dapat diharapkan memberikan manfaat sebagai berikut:

1. Bagi peneliti dan pengembang, penelitian ini memberikan referensi tambahan dalam memilih algoritma kriptografi klasik yang tepat, khususnya untuk menyeimbangkan antara keamanan dan kecepatan enkripsi dekripsi pada sistem web. Dengan mengetahui performa dan tingkat keacakan masing-masing algoritma, pengembang dapat membuat keputusan yang lebih tepat sesuai kebutuhan sistem.
2. Bagi akademis, penelitian ini menambah wawasan mengenai implementasi algoritma klasik seperti Hill Cipher dan Affine Cipher, serta pengaruhnya terhadap keamanan data dan performa sistem. Temuan ini dapat dijadikan dasar untuk penelitian lanjutan atau pengembangan metode kriptografi yang lebih efisien dan aman.