BAB I
PENDAHULUAN

1.1 Latar Belakang

Media komunikasi tentunya berkembang dari jaman ke jaman dengan berbagai tingkat keamanan yang dihadirkan. Namun, tidak ada jaminan bahwa dengan berkembangnya teknologi, berkembang pula dari segi keamanan sistemnya. Karena keamanan pada informasi atau pesan masih menjadi masalah inti di masayarakat umum dengan kebocoran data yang harusnya bersifat rahasia. Keamanan sistem merupakan keamanan pada saat pengoperasian dijalankan dalam lingkup software. Agar tetap terjaga dari segi keamanan sistem,pada informasi, terkadang perlu dilakukan dengan teknik kombinasi. Dalam media juga dibagi menjadi lima, yaitu teks, audio, video, gambar, dan protokol IP. Ada salah satu contoh data berupa teks, ialah file ekstensi dengan format .doc, .txt, .ppt, .pdf. Dalam perkembangannya , teknik penyandian pesan menjadi bahan kajian ilmu yang bernama kriptografi. Ilmu yang digunakan untuk mengamankan data dengan berbagai algoritma dan merupakan metode yang efektif untuk melindungi dari serangan pihak ketiga. Dapat dikatakan sebuah teknik yang diformulasikan secara matematik hingga mnejadi sesuatu metode yang formal.[1]

Ada dua proses dalam perangkat komunikasi yang dilindungi sistem keamanan data, yaitu melalui proses enkripsi, enkripsi dirancang untuk melindungi informasi rahasia yang dapat mengubah data dalam bentuk yang hanya dapat dicapai antara pengirim dan penerima yang dikenal sebagai deskripsi. Ada banyak metode kriptografi. Kriptografi diklasifikasikan menjadi dua jenis berdasarkan sejarahnya: kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan algoritma yang hanya menggunakan satu kunci dalam proses enkripsi dan deskripsi data. Vigenere Cipher, Caesar Cipher, dan Hill Cipher adalah tiga contoh kriptografi klasik. Pengguna kriptografi klasik jarang digunakan dalam sistem keamanan di era komputer karena tidak memiliki kesulitan yang kompleks sehingga rentan terhadap serangan. Demikian pula

kriptografi modern seperti AES, DES, ECB, dan lain-lain.[1], [2]

Penulis melakukan enkripsi menggunakan algoritma Hill Cipher dan Vigenere Cipher pada penelitian berikut. Hill Cipher adalah algoritma kunci simetris yang menggunakan matriks persegi p x p. Akibatnya, Hill Cipher termasuk dalam kelompok algoritma yang sulit dipecahkan, karena tidak menggantikan setiap alfabet dalam plaintext maupun alfabet lain yang sama dengan ciphertext, dan karena menggunakan perkalian matriks saat enkripsi dan deskripsi. . Algoritma ini memanipulasi matriks menggunakan relasi. Operasi perkalian dan invers adalah operasi matriks dasar yang digunakan. Hill Cipher adalah cipher yang sepenuhnya linier yang lebih rentan terhadap serangan.[3] Jika Vigenere Cipher adalah algoritma berbasis karakter klasik. Sebuah metode penyajian teks alfabet dengan serangkaian cipher. Algoritma ini didasarkan pada fakta bahwa itu adalah yang terbaik dalam pengkodean alfabet gabungan dan juga mudah dimengerti. Namun, di dunia sekarang ini, itu tidak lagi aman karena berbagai metode serangan lain dan kekurangannya.[4] Caesar melalui huruf kata kunci Plaintext diubah berulang kali selama proses enkripsi sampai ciphertext ditemukan. Hasilnya, ditemukan kelemahan pada pengulangan karakter yang rentan untuk dianalisis. Untuk mendukung optimalisasi keamanan informasi, diperlukan kombinasi Vigenere Cipher dan Hill Cipher.

1.2 Rumusan Masalah

Berdasar latar belakang masalah seperti di 1.1, maka bagaimana modifikasi algoritma Hill Cipher dengan Vigenere Cipher termodifikasi untuk enkripsi file dokumen ?

1.3 Batasan Masalah

Batasan dalam penelitian berikut, antara lain:

1. Penelitian menjalankan proses enkripsi dan proses deskripsi.
2. Panjang kunci terdiri dari 4 karakter.
3. Menggunakan algoritma Hill Cipher dan algoritma Vigenere Cipher.

4. Modifikasi algoritma Vigenere Cipher dalam algoritma Hill Cipher.
5. Pengimplementasian dengan bahasa pemrograman Pyhton.
6. Cakupan proses enkripsi dan proses deskripsi pada ekstensi file berupa teks dengan format txt.
7. Menggunakan matriks ordo 2x2.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah menghasilkan algoritma yang lebih kuat dengan menggabungkan algoritma Hill Cipher dan algoritma Vigenere Cipher yang di dalamnya menggunakan matriks ordo 2x2.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang telah dijabarkan, maka manfaat penelitian yang hendak digapai adalah :

1. Merancang keamanan sistem lebih ketat dalam kombinasi algoritma, sehingga pengguna dapat memberi perlindungan ekstra terhadap keamanan data dengan adanya kunci.
2. Memberi pemahaman mengenai kelemahan pada kriptografi klasik.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan meliputi :

1. **BAB I PENDAHULUAN**

   Bab ini memuat tentang latar belakang masalah, rumusan masalah, batasan penelitian, maksud dnn tujuan penelitian, metode penelitian dan sistematika penulisan.

2. **BAB II LATAR BELAKANG**

Menguraikan teori-teori yang digunakan untuk membangun sistem informasi yang dapat mendukung pengolahan data serta laporan yang berhubungan langsung dengan ilmu yang dikaji.

3. **BAB III METODOLOGI PENELITIAN**

Bab ini membahas tentang tahap-tahap penelitian yang akan dilakukan, alat dan bahan penelitian yang diperlukan, serta desain antarmuka *tool* yang digunakan.

4. **BAB IV HASIL DAN PEMBAHASAN**

Bab ini mendokumentasikan langkah-langkah penelitian yang telah dilakukan beserta hasil akhir penelitian tersebut, yang akan digunakan untuk menentukan hasil analisis dan evaluasi.

5. **BAB V PENUTUP**

Bab ini berisi kesimpulan yang ditarik dari hasil penelitianbeserta saran yang harus diperhatikan selama penelitian karena keterbatasan dalam memperoleh bahan dan rekomendasi untuk pengembangan penelitian selanjutnya.