BAB I

PENDAHULUAN

1.1 Latar Belakang

Kriptografi telah menjadi praktik penyandian yang digunakan oleh tentara Sparta di Yunani pada tahun 400 SM (Chandra, 2010). Salah satu alat sederhana yang digunakan dalam praktik ini adalah *cipher disk*, yang di mana *cipher disk* ini merupakan alat sederhana yang memungkinkan untuk mengenkripsi dan mendekripsi pesan dengan cara memutar cakram dengan huruf-huruf di atasnya, sehingga menghasilkan teks terenkripsi. Pada tahun 1467, arsitek Florentine Alberti menciptakan salah satu versi awal *cipher disk*, yang kemudian menjadi landasan untuk perkembangan teknologi penyandian selanjutnya (Aung dkk., 2019).

Salah satu pengembangan terkenal dari *cipher disk* adalah Mesin Enigma. Mesin Enigma diciptakan pada tahun 1918 oleh Arthur Scherbius (Kotas, 2000) seorang insinyur Jerman. Mesin Enigma merupakan salah satu pencapaian terbesar dalam sejarah kriptografi dan merupakan puncak dari penggunaan graf dalam kriptografi pada masa itu. Mesin Enigma bekerja dengan cara mengubah seluruh huruf pesan menjadi karakter lain melalui serangkaian putaran. Penggunaan Mesin Enigma oleh Jerman selama Perang Dunia II menimbulkan tantangan besar bagi pihak Sekutu dalam memecahkan kode-kode yang dihasilkan oleh mesin ini. Hal inilah yang menjadi cikal bakal

dalam sejarah kriptografi *modern* dengan memperkenalkan konsep kunci dan proses otomatis untuk enkripsi dan dekripsi (Weierud, 2019).

Dalam era *modern* ini kriptografi berperan sebagai pelindung informasi sensitif dan menjaga integritas serta autentikasi data. Dengan demikian, kehidupan kita akan semakin terhubung secara digital seperti komunikasi *online*, transaksi keuangan dan penyimpanan data, sehingga kriptografi sangat penting untuk memastikan keamanan sistem dan data (Hasugian, 2017). Penelitian ini menilai beberapa indikator untuk memastikan efektivitas metode kriptografi yaitu keamanan data, efisiensi metode, dan kualitas enkripsi serta dekripsi. Keamanan data mengukur kemampuan metode kriptografi dalam melindungi data dari akses tidak sah dan serangan, serta dapat dilihat dari seberapa kompleks metode kriptografi yang digunakan, di mana semakin kompleks algoritma, maka semakin sulit bagi pihak tidak berwenang untuk mendekripsi pesan tanpa kunci yang benar. Efisiensi metode mengevaluasi waktu dan sumber daya yang diperlukan untuk enkripsi dan dekripsi data. Semakin sedikit waktu yang dibutuhkan maka semakin efisien metode kriptografi tersebut, memastikan proses tidak menghambat kinerja sistem secara keseluruhan. Kualitas enkripsi dan dekripsi mengukur apakah metode tersebut dapat menghasilkan hasil dekripsi yang akurat dan konsisten dengan plainteks asli, memastikan integritas dan keandalan proses enkripsi dan dekripsi.

Peneliti memilih judul Suatu Skema Enkripsi Berbasis Graf karena skema ini menggunakan struktur graf untuk melakukan proses enkripsi dan dekripsi

data, memberikan keunggulan dalam memvisualisasikan hubungan antara kata kunci, dan hasil enkripsi (Zakin dkk., 2021). Graf adalah pasangan himpunan yang terdiri dari simpul (*nodes/vertices*), dan sisi (*edges*) dengan V adalah himpunan dan E adalah sisi. Graf dalam konteks ini menjadi representasi visual dari himpunan simpul (*nodes*) yang terhubung oleh sisi-sisi (*edges*). Pada penelitian ini, yang digunakan adalah graf bipartit. Graf bipartit adalah graf yang simpul-simpulnya terbagi menjadi dua kelompok yang terpisah dan sisi-sisinya hanya menghubungkan simpul dari kelompok yang berbeda (Liu dkk., 2021). Dalam skema kriptografi yang menggunakan graf, simpul-simpul tersebut merepresentasikan setiap karakter atau unit data. Sisi-sisi tersebut menggambarkan hubungan atau transformasi antara karakter-karakter tersebut. Dengan menggunakan graf, analisis sistem kriptografi menjadi lebih mudah, memungkinkan untuk mengidentifikasi kelemahan dan kekurangan yang mungkin ada dalam skema kriptografi. Penggunaan graf juga dapat membantu dalam mengelola dan menguji algoritma metode kriptografi baru dan metode kriptografi berbasis graf ini telah dikaji dalam beberapa penelitian terdahulu yang disusun oleh (Ghazaly, 2023).

Mengingat pentingnya menjaga keamanan data, sehingga kita harus memilih metode kriptografi yang efektif dalam menjaga keamanan data dan memiliki efisiensi yang bagus. Ada berbagai macam metode kriptografi seperti penggunaan *XOR (Exclusive OR)* yang merupakan metode manipulasi nilai biner, metode ini telah dikaji dalam penelitian sebelumnya seperti yang terdokumentasikan dalam *studi* oleh (Ghazaly, 2023) dan penelitian terdahulu

yang disusun oleh (Watrianthos, 2021). Tabel konversi *ASCII* bertujuan untuk mengubah plainteks menjadi nilai atau nilai biner (Shinge dkk., 2014). *Equation* (perhitungan matematika) yang mencakup berbagai jenis operasi seperti penjumlahan, pengurangan, perkalian, pembagian, perpangkatan, akar kuadrat dan integral pada metode ini juga dapat ditemukan pada penelitian terdahulu yang dikaji oleh (Suriadi dkk., 2020). Dalam penelitian terdahulu, menghasilkan kesimpulan bahwa metode *equation* dapat meningkatkan keamanan data. Akan tetapi, pada metode yang menggunakan penjumlahan, pengurangan, pembagian, perkalian dan lain-lain berhasil dengan sukses di mana pada hasil enkripsi yang kemudian didekripsi menggunakan kata kunci yang sama, menghasilkan hasil dekripsi yang sama dengan plainteks, sedangkan untuk penggunaan akar dan integral tidak berhasil dikarenakan pada hasil enkripsi yang kemudian didekripsi menggunakan kata kunci yang sama, menghasilkan hasil dekripsi yang berbeda dengan plainteks (Suriadi dkk., 2020)

Penelitian ini bertujuan untuk membandingkan 2 metode kriptografi dalam upaya untuk meningkatkan keamanan data. Metode yang digunakan yaitu metode kriptografi yang dibuat penulis dengan menggunakan tabel konversi berdasarkan tabel *ASCII* yang bertujuan untuk mengubah plainteks menjadi nilai agar mempermudah dalam menerapkan kriptografi *modern*, dengan penggunaan kata kode untuk modifikasi, serta melakukan pemisahan kata kode menjadi 2 sub kata kode yaitu sub kata kode kanan dan kiri, dengan tujuan untuk pembuatan graf yang di mana selanjutnya metode ini diberi nama metode

1. Metode ini dibandingkan dengan metode kriptografi lainnya, yang dikembangkan berdasarkan metode 1 dengan melakukan penambahan *equation* pada sub kata kode kanan yang selanjutnya metode ini diberi nama metode 2. Pemilihan metode *equation*, dikarenakan mudah untuk diimplementasikan dan dapat meningkatkan kompleksitas, sehingga membuatnya lebih sulit bagi pihak yang tidak berwenang untuk mendekripsi pesan yang telah dienkripsi dan dapat digabungkan ke dalam berbagai jenis metode kriptografi sehingga metode ini lebih *fleksibel*.

Penelitian ini sangat penting untuk dilakukan, dikarenakan meningkatnya ancaman terhadap keamanan data yang disebabkan oleh tersebarnya data di berbagai *database* dan kurangnya keamanan dari *database* yang menyimpan data, sehingga *hacker* mudah untuk meretas dan mencuri data. Sebagai contoh, kasus peretasan yang dilakukan oleh kelompok Surabaya *Black Hat* (SBH), yang telah meretas lebih dari 600 situs *web* yang tersebar di 44 negara pada tahun 2018 (Shelley, 2019). Dengan pembuatan metode kriptografi dan melakukan perbandingan antara 2 buah metode kriptografi, penelitian ini bertujuan untuk mengevaluasi efisiensi dan kecepatan masing-masing pendekatan, serta untuk memahami keunggulan dan kelemahan yang terkait dengan penggunaan struktur graf dan operasi matematika atau logika dalam kriptografi.

Hasil dari penelitian ini, diharapkan dapat memberikan pemahaman yang lebih baik tentang kelebihan dan kekurangan masing-masing metode kriptografi, serta memberikan panduan dalam pemilihan metode kriptografi

yang sesuai dengan kebutuhan keamanan data di era digital saat ini. Dengan demikian, penelitian ini dapat memberikan kontribusi yang signifikan, dalam pengembangan teknologi kriptografi, yang lebih canggih dan andal untuk mengamankan data yang kita miliki.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian adalah:

1. Bagaimana algoritma kriptografi dari metode 1 dan 2?
2. Bagaimana perbandingan efisiensi dari kriptografi metode 1 dan 2?
3. Bagaimana perbandingan keamanan dari kriptografi metode 1 dan 2?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1 Menjelaskan agoritma kriptografi dari metode 1 dan 2.

2 Menganalisis perbandingan efisiensi kriptografi metode 1 dan 2.

3 Mengevaluasi perbandingan keamanan kriptografi metode 1 dan 2.

1.4 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh yakni :

1 Manfaat Teoritis

Terdapat manfaat teori yang diharapkan oleh peneliti, yaitu dapat melaksanakan penelitian dengan memberikan sumbangsih pemikiran dan, menambah kasanah ilmu pengetahuan dalam bidang kriptografi.

2 Manfaat Praktis

a. Bagi Peneliti

Untuk meningkatkan pemahaman serta ilmu pengetahuan dalam mengkaji permasalahan mengenai penggunaan metode kriptografi, bertujuan untuk lebih meningkatkan keamanan, dan mendapatkan pengalaman dalam melaksanakan penelitian karya ilmiah, serta dapat mengaplikasikan ilmu kriptografi yang telah dipelajari.

b. Bagi Pembaca

Dapat menambah wawasan, dan dapat digunakan sebagai referensi mengenai penggunaan kriptografi beserta langkah-langkahnya.

c. Bagi Pemerintah

Pada hasil penelitian ini, diharapkan dapat memberikan manfaat untuk dunia pendidikan, pemerintahan, dan pengembang aplikasi, sehingga penelitian ini dapat menjadi salah satu bahan masukkan pengambilan kebijakan untuk memilih atau menggabungkan metode kriptografi dalam upaya meningkatkan keamanan.

1.5 Batasan Masalah

Agar dalam pembahasan tidak terlalu luas dan hasilnya dapat mendekati pokok permasalahan, maka terdapat batasan masalah dalam penelitian ini yaitu, membandingkan antara kedua metode yang melibatkan evaluasi berdasarkan waktu yang diperlukan untuk proses enkripsi dan dekripsi, dan tingkat keamanan yang dilihat dari kompleksitas, serta efisiensi yang dinilai dari panjang simpul pada graf yang digunakan.


UNIVERSITAS PENDIDIKAN GANESHA
UNDIKSHA