BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Perkembangan teknologi informasi dan komunikasi telah mengalami kemajuan yang signifikan dan memainkan peran penting dalam berbagai aspek kehidupan manusia. Salah satu aspek krusial dari teknologi informasi adalah kemampuannya untuk memfasilitasi komunikasi dan pertukaran informasi antar individu dengan cepat dan efisien. Di era globalisasi dan digitalisasi yang semakin pesat, penggunaan teknologi untuk mengirim pesan teks melalui berbagai platform komunikasi telah menjadi bagian dari kehidupan sehari-hari.

Platform komunikasi digital seperti email, pesan instan, media sosial, dan aplikasi obrolan telah menggantikan banyak metode komunikasi tradisional. Dengan teknologi ini, individu dapat mengirim pesan dan informasi ke berbagai belahan dunia dalam hitungan detik, mempercepat arus informasi, dan memungkinkan kolaborasi yang lebih efektif. Teknologi ini juga memungkinkan seseorang untuk tetap terhubung dengan keluarga, teman, dan rekan kerja tanpa batasan geografis (Asari et al, 2019).

Selain keunggulan teknologi tersebut, keamanan informasi juga merupakan aspek yang sangat penting. Seiring dengan perkembangan teknologi dan meningkatnya jumlah data yang ditransmisikan dan disimpan secara digital, ancaman terhadap keamanan data juga menjadi semakin kompleks. Dalam konteks ini, kriptografi memegang peran penting dalam melindungi informasi dari akses tidak sah. Salah satu teknik kriptografi yang banyak digunakan adalah *block cipher*, yang mengenkripsi data dalam blok-blok berukuran tetap. Menurut Munir (2019), *block cipher* adalah bagian dari kriptografi modern di mana bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang yang sama. Proses enkripsi dilakukan terhadap blok plainteks menggunakan bit-bit kunci. Sebuah kunci dapat berupa angka atau kombinasi dari angka, karakter, dan simbol spesial. Kunci ini digunakan baik untuk mengenkripsi plainteks maupun mendekripsi cipherteks. Kunci juga berperan penting dalam menentukan kekuatan keamanan sistem enkripsi kriptografi.

Kekuatan keamanan tersebut bergantung pada keacakan dan panjang kunci. *Avalanche Effect* dan koefisien korelasi sering digunakan untuk mengukur keamanan algoritma kriptografi. *Avalanche Effect* merujuk pada keadaan di mana perubahan kecil dalam *input* (seperti mengubah satu bit dari plainteks atau kunci) menghasilkan perubahan besar dalam *output* (cipherteks). Sedangkan koefisien korelasi mengacu pada hubungan statistik antara variabel-variabel dalam sistem kriptografi. Hasil korelasi yang rendah antara plainteks, cipherteks, dan kunci sangat diharapkan, karena mengurangi kemungkinan pola dalam plainteks atau kunci dikenali dalam cipherteks.

Terdapat beberapa penelitian terkait yang menggunakan teknik *block cipher* untuk mengamankan pesan teks. Penelitian yang dilakukan oleh Fauzi et al. (2021) merancang algoritma kriptografi *block cipher* berdasarkan pola *dribbling practice*. Penelitian ini menggunakan metode seperti S-box, jaringan *Feistel*, operasi XOR, dan pergeseran kunci sandi dengan spesifikasi algoritma enkripsi sebesar 15 putaran enkripsi. Putaran enkripsi adalah jumlah perulangan di mana data plainteks dienkripsi oleh suatu algoritma kriptografi. Hasil penelitian tersebut menunjukkan *Avalanche Effect* sebesar 54,687% dan nilai rata-rata koefisien korelasi sebesar 0,24. Penelitian serupa dilakukan oleh Kumbara et al. (2019), yang juga menggunakan teknik *block cipher* untuk membuat algoritma kriptografi, namun menggunakan empat pola berbeda yang diambil dari permainan tradisional Rangku Alu. Penelitian ini menghasilkan nilai *Avalanche Effect* sebesar 49,38% dan nilai rata-rata koefisien korelasi sebesar 0,18 dengan 10 putaran enkripsi. Selain itu, penelitian oleh Aziiz et al. (2019) juga membuat algoritma kriptografi *block cipher* menggunakan pola batik ceplok Yogyakarta sebagai dasar algoritma. Penelitian ini menghasilkan nilai *Avalanche Effect* sebesar 47,656% dengan nilai rata-rata koefisien korelasi sebesar 0,39 dan 10 putaran enkripsi. Algoritma enkripsi yang kuat harus memenuhi beberapa kriteria, antara lain memiliki prinsip *confusion* dan *diffusion*. Prinsip *confusion* menyembunyikan hubungan antara plainteks, cipherteks, dan kunci, prinsip *confusion* berkaitan erat dengan definisi koefisien korelasi. Koefisien korelasi yang baik untuk algoritma kriptografi harus mendekati 0, yang berarti antara plainteks dan

cipherteks tidak ditemukan adanya korelasi. Prinsip *diffusion* menyebarkan pengaruh satu bit plainteks atau kunci ke sebanyak mungkin cipherteks, sesuai dengan definisi *Avalanche Effect*. Nilai *Avalanche Effect* yang baik harus berkisar antara 45% hingga 60% dengan kriteria sangat baik di 50% (Echeverri, 2017). Meskipun hasil dari penelitian terdahulu menunjukkan nilai koefisien korelasi dan *Avalanche Effect* yang cukup baik, semua algoritma enkripsi yang diteliti tersebut menggunakan pola dan putaran enkripsi yang statis. Hal ini membuat algoritma tersebut rentan terhadap beberapa jenis serangan, seperti serangan *brute force* atau analisis kriptografi.

Penelitian Perancangan Algoritma Kriptografi Block Cipher Berbasis Permainan Pola Catur Sebagai Kunci Dinamis dilakukan sebagai pembaruan dari penelitian sebelumnya. Dalam penelitian ini, permainan catur dimanfaatkan sebagai *generator* pola enkripsi yang dinamis. Permainan catur menawarkan kompleksitas tinggi dengan jutaan kombinasi langkah yang mungkin dilakukan. Setiap langkah dalam catur dianggap sebagai pola unik dan dinamis. Menggunakan bidak catur untuk menghasilkan pola langkah sebagai dasar pembangkitan kunci dinamis dalam algoritma kriptografi merupakan pendekatan inovatif yang belum banyak dieksplorasi. Pola langkah dari permainan catur memberikan keragaman dan dinamika dalam pembentukan kunci kriptografi, yang secara langsung meningkatkan tingkat keamanan algoritma enkripsi. Pola langkah catur ini direncanakan akan digunakan sebagai kunci kedua (kunci 2) dalam algoritma kriptografi ini. Dengan menggabungkan kunci 1 berupa 8 karakter ASCII dengan kunci 2 yang merupakan pola langkah catur, diharapkan algoritma ini dapat menghasilkan cipherteks yang sulit untuk ditebak, dan secara signifikan meningkatkan keamanan data yang dienkripsi.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang permasalahan yang sudah dijelaskan di atas, maka dapat dirumuskan permasalahannya adalah:

1. Bagaimana merancang algoritma *block cipher* yang memanfaatkan pola langkah bidak catur sebagai kunci dinamis?

2. Bagaimana meningkatkan keamanan dalam pengiriman pesan teks menggunakan metode kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis?
3. Bagaimana merancang dan membangun aplikasi *website* dengan menerapkan metode kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah penelitian di atas, maka tujuan dari penelitian ini adalah:

1. Merancang algoritma kriptografi *block cipher* berbasis pola catur.
2. Meningkatkan keamanan dalam pengiriman pesan teks menggunakan metode kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis.
3. Merancang dan membangun aplikasi *website* dengan menerapkan metode kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis.

1.4 Batasan Penelitian

Terdapat batasan penelitian yang ditetapkan pada penelitian ini. Adapun batasan penelitian tersebut adalah:

1. *Input* kunci 2 pada aplikasi *website* masih dapat di isi oleh kombinasi langkah catur acak.
2. Aplikasi catur belum di integrasikan pada aplikasi *website*.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian di atas, manfaat yang ingin diperoleh dari penelitian ini adalah sebagai berikut:

1. Memberikan inovasi baru dalam pengembangan algoritma kriptografi *block cipher* dengan memanfaatkan pola langkah catur sebagai kunci dinamis, yang belum banyak diteliti sebelumnya.
2. Meningkatkan keamanan informasi dengan memperkenalkan metode enkripsi yang menggunakan kunci dinamis berbasis langkah catur.

3. Menjadi referensi bagi penelitian lanjutan dalam bidang kriptografi dan memberikan perspektif baru mengenai penggunaan pola langkah catur sebagai kunci dinamis dalam algoritma enkripsi.
4. Hasil penelitian ini dapat diimplementasikan dalam berbagai aplikasi praktis yang membutuhkan keamanan tinggi, seperti komunikasi data, penyimpanan informasi sensitif, dan sistem keamanan siber.

1.6 Struktur Organisasi Skripsi

Struktur organisasi mencakup deskripsi penulisan penelitian dari awal sampai akhir yang terdiri dari 5 bab. Setiap bab memiliki bagian-bagian struktur organisasi yang diuraikan sebagai berikut:

Bab I Pendahuluan, mencakup latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian, dan struktur penulisan.

Bab II Kajian Pustaka, mencakup teori dan studi literatur terkait kriptografi, prinsip *Shannon*, metode *Substitution Box*, metode transposisi bit *cipher*, uji *Avalanche Effect*, uji korelasi, uji *Brute Force Atack*, permainan catur, dan penelitian terkait.

Bab III Metode Penelitian, mencakup desain penelitian dan rincian metode penelitian yang digunakan pada penelitian ini.

Bab IV Temuan dan Pembahasan, mencakup hasil penelitian terkait perancangan algoritma kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis.

Bab V Simpulan, Implikasi, dan Rekomendasi, mencakup kesimpulan, implikasi, dan rekomendasi dari hasil penelitian terkait perancangan algoritma kriptografi *block cipher* berbasis permainan pola catur sebagai kunci dinamis.