# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

*Advanced Encryption Standard* (AES) merupakan algoritma enkripsi simetris berbasis block cipher yang telah menjadi salah satu standar utama dalam perlindungan data digital. Menurut NIST (2023), AES ditetapkan sebagai algoritma kriptografi yang dapat digunakan untuk melindungi data elektronik, dengan ukuran blok tetap 128 bit. AES masih memiliki relevansi tinggi dalam implementasi keamanan informasi modern, salah satunya difusi pada *ciphertext*, Kemudian dalam penerapannya, penggunaan AES tidak terbatas pada kajian teoretis kriptografi, tetapi juga digunakan secara luas dalam berbagai sistem nyata yang membutuhkan perlindungan kerahasiaan data, seperti sistem komunikasi jaringan, penyimpanan data, enkripsi dokumen, aplikasi berbasis cloud, dan sistem informasi modern (Ganesh dkk., 2025).

Peningkatan kecepatan enkripsi merupakan kebutuhan fundamental dalam kriptografi modern. Sistem keamanan informasi tidak hanya dituntut untuk menghasilkan *ciphertext* yang aman, tetapi juga harus mampu memproses data dengan efisien untuk menjaga responsivitas sistem keseluruhan. Komputasi yang lambat pada proses enkripsi dapat menjadi *bottleneck* dalam pipeline pemrosesan data dan meningkatkan latensi sistem. Oleh karena itu, optimasi algoritma kriptografi untuk mencapai performa yang lebih baik tanpa mengorbankan kualitas difusi merupakan penelitian yang selalu relevan dan diperlukan dalam

pengembangan praktis kriptografi (Ganesh dkk., 2025). Namun, optimasi kecepatan enkripsi harus diimbangi dengan mempertahankan kualitas difusi *ciphertext*, karena difusi merupakan salah satu prinsip fundamental dalam kriptografi modern. Difusi *ciphertext* bertujuan menyebarkan pengaruh perubahan kecil pada plaintext atau kunci ke seluruh bagian *ciphertext* sehingga pola asli data sulit dikenali. Kualitas difusi yang kuat mampu meningkatkan resistansi algoritma terhadap serangan statistik maupun diferensial, karena perubahan satu bit pada input akan menyebar ke banyak bit output *ciphertext*, sehingga kriptanalis tidak dapat menemukan hubungan statistik antara plaintext dan *ciphertext* (Li dkk., 2024).

Optimasi kecepatan enkripsi melalui pengurangan jumlah *round* atau penggantian fungsi transformasi berpotensi menurunkan kualitas difusi. Penelitian sebelumnya menunjukkan bahwa pengurangan *round* tanpa mekanisme kompensasi difusi yang memadai dapat menurunkan *Avalanche effect* dan entropi *ciphertext*, sehingga algoritma menjadi lebih rentan terhadap analisis pola statistik. Dengan demikian, peningkatan kecepatan enkripsi perlu dilakukan tanpa mengorbankan prinsip difusi, yaitu dengan merancang mekanisme transformasi yang tetap mampu menyebarkan pengaruh perubahan pada input ke seluruh bagian *ciphertext* meskipun jumlah operasinya lebih sedikit.

Sejumlah penelitian telah mengidentifikasi bahwa AES memiliki kelemahan dari sisi komputasi, khususnya pada fungsi *MixColumns*. Penelitian yang dilakukan pada tahun 2020 menyatakan bahwa *MixColumns* merupakan transformasi yang paling berat secara komputasi dalam AES karena melibatkan operasi perkalian dan

penjumlahan yang kompleks dalam *Galois Field*, sehingga menyebabkan proses enkripsi berjalan lambat (Gamido, 2020). Sebagai solusi, Penelitian tersebut mengusulkan penggantian fungsi *MixColumns* dengan teknik *bit permutation*. Pendekatan ini terbukti berhasil meningkatkan kecepatan enkripsi sekaligus menghasilkan *Avalanche effect* yang lebih tinggi dibandingkan AES standar. Penelitian tersebut kemudian dikembangkan lebih lanjut dengan menggabungkan penggantian *MixColumns* dengan pengurangan jumlah *round* dari sepuluh menjadi enam, menghasilkan peningkatan kecepatan enkripsi sebesar 76,76% dan dekripsi sebesar 55,46% dengan *Avalanche effect* 52,92% yang melampaui batas minimum *Strict Avalanche Criterion (SAC)* sebesar 50% (Baladhay & De Los Reyes, 2024).

Namun demikian, pendekatan tersebut masih memiliki keterbatasan pada mekanisme tabel permutasi yang digunakan. Tabel permutasi pada penelitian sebelumnya masih bersifat *fixed*, yaitu menggunakan urutan indeks yang tetap dan sama untuk setiap proses enkripsi, tanpa bergantung pada kunci yang digunakan. Kondisi ini membuat pola permutasi tidak berubah meskipun kunci enkripsi berbeda. Oleh karena itu, penelitian ini diarahkan untuk mengembangkan mekanisme *bit permutation* yang bersifat dinamis dan bergantung pada kunci, sehingga tabel permutasi yang digunakan dapat berubah sesuai kunci enkripsi tanpa mengubah fokus utama penelitian, yaitu peningkatan kecepatan enkripsi dan pemertahanan kualitas difusi *ciphertext*. Salih dkk. (2020) sendiri telah menyelesaikan masalah statis pada *MixColumns* dengan membuatnya dinamis menggunakan 3D *Chebyshev chaotic map*. Namun, pendekatan tersebut tetap

mempertahankan *MixColumns* yang secara inheren memiliki beban komputasi tinggi akibat operasi *Galois Field*, sehingga masalah kecepatan tidak terselesaikan.

Terdapat celah penelitian yang belum dijembatani, Baladhay (2024) berhasil meningkatkan kecepatan dengan mengganti *MixColumns* menggunakan *bit permutation*, namun tabel permutasinya bersifat statis, di sisi lain, Salih dkk. (2020) berhasil membuat komponen AES menjadi dinamis berbasis *chaotic map*, namun tidak mengganti *MixColumns*. Berdasarkan studi literatur yang berhasil diidentifikasi, belum ditemukan penelitian yang secara simultan menggabungkan penggantian *MixColumns* menggunakan *bit permutation* yang bersifat dinamis, bergantung pada kunci enkripsi, serta dibangkitkan menggunakan pendekatan *chaotic map* pada AES *reduced-round*.

Penelitian ini mengusulkan modifikasi algoritma AES-128 untuk meningkatkan kecepatan enkripsi tanpa mengurangi kualitas difusi *ciphertext* melalui penerapan *reduced round* dan *dynamic key-dependent bit permutation* berbasis *logistic chaotic map*. Tabel permutasi pada pendekatan tersebut dibangkitkan secara dinamis menggunakan kunci enkripsi sebagai parameter awal, sehingga setiap kunci menghasilkan pola permutasi yang berbeda. Perbedaan pola tersebut diharapkan dapat meningkatkan ketergantungan algoritma terhadap kunci dan mendukung proses difusi *ciphertext*, yang dievaluasi melalui *Avalanche effect*, entropi Shannon, dan *Key sensitivity*. Potensi *overhead* dari pembangkitan tabel permutasi dinamis dikendalikan melalui penerapan *reduced round* sebagai strategi kompensasi komputasi. Mekanisme *dynamic key-dependent bit permutation* membutuhkan tahap tambahan berupa SHA-256, *logistic chaotic map*, dan *Fisher-Yates shuffle*,

sehingga jumlah *round* AES dikurangi dari 10 menjadi 6 agar beban komputasi total tetap ringan. Selain itu, tabel permutasi tidak dibangkitkan pada setiap blok atau setiap *round*, melainkan hanya satu kali pada tahap pra-proses untuk setiap kunci enkripsi. Setelah terbentuk, tabel disimpan sementara di memori dan digunakan kembali untuk seluruh blok data dengan kunci yang sama. Kontribusi penelitian ini terletak pada integrasi keunggulan kecepatan dari pendekatan Baladhay dan De Los Reyes (2024) dengan keunggulan dinamisme berbasis *chaotic map* dari Salih dkk. (2020), sehingga diperoleh rancangan AES-128 termodifikasi yang lebih efisien sekaligus memiliki pola permutasi yang dinamis dan bergantung pada kunci.

*Advanced Encryption Standard* (AES) adalah algoritma kriptografi simetris yang dirancang sebagai block cipher, memproses data dalam blok-blok tetap 128 bit. Sebagai block cipher, AES mengolah aliran data byte secara paralel per blok. oleh karena itu, struktur internal teks atau file lain tidak memengaruhi mekanisme enkripsi dasar. Konsekuensinya, setiap jenis file diurai menjadi blok-bit yang serupa sebelum dilakukan enkripsi (Limartha & Wibawa, 2025). Penggunaan file teks berformat .txt dinilai memadai untuk pengujian awal karena AES memproses data sebagai rangkaian byte tanpa bergantung pada jenis atau format berkas. Oleh karena itu, file .txt dapat merepresentasikan proses enkripsi sebagaimana format berkas lainnya. Ukuran file yang digunakan dalam pengujian meliputi 10 KB, 20 KB, 30 KB, 40 KB, 50 KB, 100 KB, dan 1 MB.

Pemilihan ukuran file uji sebesar 10 KB, 20 KB, 30 KB, 40 KB, 50 KB, 100 KB, dan 1 MB dilakukan untuk mengevaluasi performa algoritma AES-128 termodifikasi pada jumlah blok data yang berbeda. Pemilihan ukuran tersebut

mengacu pada pola pengujian performa enkripsi dalam penelitian terdahulu. Mioc dan Pentiuc (2015) menggunakan variasi ukuran file mulai dari 10 KB, 20 KB, 30 KB, 40 KB, 50 KB, 100 KB, hingga 1 MB dalam pengujian perbandingan algoritma AES, Camellia, dan SEED (Mioc & Pentiuc, 2015). Selain itu, Saputra dkk. (2025) juga menggunakan variasi ukuran data 1 KB, 10 KB, 100 KB, dan 1 MB untuk mengevaluasi stabilitas dan skalabilitas proses enkripsi-dekripsi pada model berbasis AES (Saputra dkk., 2025). Dengan demikian, ukuran 10 KB sampai 50 KB digunakan untuk merepresentasikan file kecil, 100 KB digunakan sebagai ukuran transisi menuju file menengah, sedangkan 1 MB digunakan untuk menguji skalabilitas algoritma ketika jumlah blok yang diproses meningkat lebih besar. Variasi ukuran ini diperlukan agar pengaruh ukuran file terhadap kecepatan enkripsi, kecepatan dekripsi, *Throughput* , *Avalanche effect*, entropi Shannon, *Key sensitivity*, *Frequency test*, *Runs test*, dan *Chi-Square test* dapat diamati secara lebih terukur dan dapat dibandingkan dengan penelitian terdahulu.

## 1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, dapat dirumuskan masalah pada penelitian ini, yaitu:

a. Bagaimana merancang mekanisme *bit permutation* yang bersifat dinamis dan bergantung pada kunci enkripsi sehingga mengurangi keterbatasan tabel permutasi statis?
b. Bagaimana pengaruh penerapan *reduced round* dan dynamic *key-dependent bit permutation* berbasis *logistic chaotic map* terhadap trade-off antara kecepatan komputasi dan kualitas difusi *ciphertext* pada AES-128?

## 1.3 Tujuan Penelitian

Berdasarkan uraian masalah yang sudah dirumuskan, didapat tujuan penelitian sebagai berikut:

*a.* Mengimplementasikan modifikasi algoritma AES-128 dengan *reduced round* dan penggantian fungsi *MixColumns menggunakan dynamic key-dependent bit permutation* berbasis *logistic chaotic map.*

*b.* Mengevaluasi pengaruh *reduced round* dan *dynamic bit permutation* terhadap kecepatan dan kualitas difusi *ciphertext* ditinjau dari Kecepatan Enkripsi, Kecepatan Dekripsi, *Avalanche effect*, *Throughput ,* Entropi Shannon, *Key sensitivity, Frequency test, Runs test, dan Chi-Square test.*

## 1.4 Manfaat Penelitian

Beberapa manfaat yang didapatkan dari penelitian ini, sebagai berikut:

a. Memberikan kontribusi dalam kajian modifikasi AES-128, khususnya pada penerapan *dynamic key-dependent bit permutation* berbasis *logistic chaotic map* sebagai alternatif pengganti *MixColumns* yang lebih ringan secara komputasi.

b. Menghasilkan *proof of concept* algoritma AES-128 yang dimodifikasi dalam bentuk implementasi perangkat lunak yang dapat dijadikan referensi bagi peneliti selanjutnya.

## 1.5 Batasan Masalah

Berikut merupakan batasan masalah yang terdapat pada penelitian ini:

a. Algoritma yang dimodifikasi dalam penelitian ini hanya mencakup AES-128 dengan panjang kunci 128 bit.
b. Modifikasi yang dilakukan dalam penelitian ini mencakup penggantian fungsi *MixColumns* dengan mekanisme *dynamic key-dependent bit permutation* berbasis *logistic chaotic map* serta pengurangan jumlah *round* AES-128 dari 10 *round* menjadi 6 *round*.
c. Pengujian algoritma hanya dilakukan pada enkripsi data dalam bentuk file .txt dengan panjang bervariasi, yaitu 10KB, 20KB, 30KB, 40KB, 50KB, 100KB, dan 1MB.
d. Evaluasi performa algoritma dibatasi pada sembilan metrik kuantitatif yaitu Kecepatan Enkripsi, Kecepatan Dekripsi, *Avalanche effect*, *Throughput* , Entropi Shannon, *Key sensitivity, Frequency test, Runs test, dan Chi-Square test*.
e. Penelitian tidak menguji serangan kriptanalis diferensial/linear secara formal.

## 1.6 Sistematika Penulisan

Penelitian ini menggunakanvsistematika penulisan yang terdiri dari 5 BAB, sistematika penulisan yang digunakan meliputi:

**BAB I Pendahuluan**

Berisi tentang Latar Belakang, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, Batasan Masalah, dan Sistematika Penulisan.

**BAB II Tinjauan Pustaka**

Berisi Landasan teori yang memuat teori relevan terhadap penelitian, *State of the art* yang memuat penelitian sebelumnya serta hasil penelitian sebelumnya yang relevan terhadap penelitian ini

**BAB III Metodologi Penelitian**

Menjelaskan mengenai metode yang diterapkan pada penelitian ini, mencakup road*map* penelitian serta rincian prosedur setiap tahapan penelitian.

**BAB IV Hasil dan Pembahasan**

Me*map*arkan dan menganalisis hasil penelitian, analisis data, evaluasi model hingga mendapatkan hasil akhir dari penelitian yang dilakukan

**BAB V Penutup**

Berisi kesimpulan akhir dari penelitian yang dilakukan dan saran-saran yang direkomendasikan oleh peneliti berdasarkan pengalaman yang telah dilalui sebagai perbaikan untuk penelitian selanjutnya.