BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi saat ini memungkinkan orang untuk berkomunikasi dan berbagi data serta informasi tanpa terhalang oleh jarak atau waktu. Seiring dengan meningkatnya kebutuhan akan keamanan dalam menjaga kerahasiaan informasi yang dibagikan, permintaan terhadap ketersediaan data dan sistem keamanan informasi yang lebih andal semakin meningkat untuk melindungi data dari risiko pencurian. Oleh karena itu, pengembangan metode pembelajaran ilmiah untuk melindungi data menjadi salah satu dampak positif dari keberadaan sistem keamanan yang dirancang guna menjaga data yang dikirimkan melalui jaringan komunikasi.(Azhari et al., 2022) Berbagai jenis serangan siber seperti pencurian data, pemalsuan data, dan akses ilegal. Kriptografi memberikan peran penting dalam melindungi *file* dokumen dengan menjaga kerahasiaan, integritas dan otentikasi data. Dengan menggunakan algoritma kriptografi, *file* dapat dienkripsi sedemikian rupa. Enkripsi merupakan proses mengubah teks yang mudah dipahami (*plaintext*) menjadi teks yang tidak dapat dipahami (*ciphertext*).(Wachid Hidayatulloh et al., 2023)

Dengan kemajuan teknologi komputasi kuantum, ancaman terhadap sistem kriptografi konvensional semakin nyata. Komputer kuantum memiliki potensi untuk merusak sistem kriptografi kunci publik yang banyak digunakan, seperti RSA dan AES, melalui algoritma seperti algoritma Shor. Kemampuan ini menimbulkan risiko signifikan terhadap keamanan data, karena informasi yang dienkripsi hari ini dapat dipecahkan di masa depan oleh komputer kuantum yang cukup kuat. Akibatnya, kriptografi Post-Quantum Cryptography (PQC) sedang dieksplorasi karena kebutuhan akan sistem kriptografi dengan keamanan tinggi yang dapat menahan serangan kuantum. (Anastasova et al., 2022)

Algoritma Twofish merupakan algoritma yang diakui sebagai algoritma dengan tingkat efesiensi dan keamanan yang tinggi dibandingkan dengan algoritma simetris lainnya. Algoritma ini juga lebih efisien dalam perangkat keras dan

perangkat lunak, terutama untuk perangkat dengan sumber daya terbatas. Algoritma Twofish merupakan algoritma kriptografi kunci simetrik cipher blok dengan panjang blok tetap 128-bit.(Kurniawan et al., 2024) Algoritma ini menggunakan jaringan Feistel 16 putaran dan 4 kotak-S yang bergantung pada *key*, serta mendukung kunci hingga 256-bit, menjadikannya pilihan yang kuat untuk enkripsi data.(Siswanto et al., 2021)

Di sisi lain, kriptografi asimetris, seperti *Kyber Key Encapsulation Mechanism* (KEM), menawarkan keamanan yang lebih baik dalam hal manajemen pengelolaan kunci. *Kyber Key Encapsulation Mechanism* (Kyber KEM) merupakan salah satu kandidat terkemuka dalam standardisasi post-quantum cryptography oleh NIST (*National Institute of Standards and Technology*), yang dirancang untuk menghadapi ancaman komputasi kuantum. Salah satu sifat keamanan paling penting dari Kyber, seperti yang dievaluasi oleh NIST, adalah kemampuannya untuk memberikan IND-CCA *security*, yaitu perlindungan terhadap serangan *ciphertext* terpilih adaptif. Dalam aplikasi modern seperti *cryptocurrencies*, *broadcast encryptio*n, and *auction protocols*, diperlukan tingkat keamanan tambahan di luar IND-CCA, seperti *anonymity*. Ini berarti bahwa *ciphertext* tidak boleh membocorkan informasi tentang kunci publik yang digunakan untuk enkripsi. Pada awalnya, Kyber mengalami kesulitan dalam membuktikan kemampuannya untuk menjaga *anonymity* karena kendala teknis. Namun, penelitian terbaru telah berhasil mengatasi masalah ini dan membuktikan bahwa Kyber juga dapat memberikan keamanan ANO-CCA, yang memastikan skema tetap anonim meskipun ada serangan ciphertext terpilih.(Maram & Xagawa, 2023)

Penggabungan algoritma Twofish dan Kyber KEM dalam implementasi *hybrid encryption* menjadi penting karena kedua algoritma ini menawarkan keunggulan yang saling melengkapi dalam konteks keamanan informasi. Penggabungan kedua algoritma tersebut menciptakan sistem yang menggabungkan kecepatan dan efisiensi dari kriptografi simetris dengan keamanan yang tangguh terhadap serangan kuantum dari kriptografi asimetris. Dalam pendekatan ini, Kyber berperan menghasilkan *shared secret key* yang dimanfaatkan sebagai kunci pada algoritma enkripsi simetris Twofish. Pendekatan *hybrid* ini menggabungkan kecepatan dan efisiensi enkripsi simetris dengan tingkat keamanan tinggi dalam pengelolaan kunci

yang ditawarkan oleh Kyber, sehingga data tetap aman meski menghadapi ancaman komputasi kuantum.

Berdasarkan latar belakang diatas, Penelitian ini mengusulkan implementasi *hybrid encryption* yang menggabungkan Twofish sebagai algoritma simetris untuk mengenkripsi *file* dokumen dan Kyber KEM sebagai manajemen pengelolaan kunci dengan metode *encapsulation mechanism*. Dengan menggabungkan dua algoritma ini , diharapkan dapat memberikan solusi tidak hanya cepat dan efisien, namun juga memberikan solusi keamanan data yang lebih baik di era komputasi kuantum yang semakin canggih dan diprediksi menjadi ancaman besar di masa depan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat dirumuskan beberapa permasalahan dalam penelitian ini sebagai berikut:

1. Bagaimana implementasi sistem *Hybrid Encryption* yang mengintegrasikan algoritma Twofish dan Kyber KEM?
2. Bagaimana analisa performa dari sistem *Hybrid Encryption* yang diimplementasikan?

1.3. Tujuan Penelitian

Tujuan Penelitian ini sebagai berikut :

1. Mengembangkan sistem *Hybrid Encryption* yang mengintegrasikan algoritma Twofish dan Kyber KEM.
2. Menganalisis performa dari sistem *Hybrid Encryption* yang diimplementasikan, termasuk waktu proses enkripsi, waktu proses dekripsi, dan kecepatan.

1.4. Batasan Masalah

Penelitian ini memiliki beberapa batasan untuk menjaga fokus dan keterarahan studi. Pertama, penelitian hanya mencakup keamanan *file* dokumen dalam format Word dan PDF dengan ukuran dokumen yang dibatasi hanya 10 MB, sehingga jenis *file* gambar, video, atau format dokumen lainnya tidak dibahas. Kedua, pada analisis performa, penelitian ini terbatas pada waktu proses enkripsi, waktu proses dekripsi, kecepatan enkripsi dan kecepatan dekripsi.

1.5. Manfaat Penelitian

1. Bagi peneliti lain yang bergerak dalam bidang kriptografi, penelitian ini menjadi salah satu yang memberikan kontribusi dalam menjelaskan pengembangan model *hybrid encryption* terutama untuk algoritma Twofish dan Kyber KEM.
2. Bagi peneliti yang ingin mengeksplorasi atau mengembangkan sistem enkripsi hybrid, penelitian ini dapat dijadikan acuan dalam menghadapi tantangan keamanan akibat ancaman komputasi kuantum.

1.6. Sistematika Penulisan

Untuk memberikan penjelasan yang terstruktur, sistematika penulisan dalam dokumen ini disusun sebagai berikut:

1. Bab I Pendahuluan:

   Bab ini Menguraikan latar belakang masalah, perumusan masalah, tujuan penelitian, batasan masalah, dan manfaat penelitian.
2. Bab II Kajian Pustaka:

   Bab ini Menyajikan penjelasan singkat penelitian terdahulu dan tinjauan literatur yang relevan dengan penelitian, termasuk pembahasan algoritma Twofish, Kyber *Key Encapsulation Mechanism*, konsep *hybrid encryption* dan alasan pemilihan teori.
3. Bab III Metodologi Penelitian:

   Bab ini Membahas jenis penelitian, desain penelitian, tahapan implementasi sistem hybrid encryption, dan analisis data.
4. Bab IV Pembahasan:

   Bab ini menjelaskan tahapan implementasi sistem *Hybrid Encryption* yang mengintegrasikan algoritma Twofish dan Kyber KEM, termasuk struktur program dan cara kerja sistem. Selain itu, bab ini juga memaparkan hasil pengujian terhadap sistem yang telah dibangun, seperti waktu proses enkripsi dan dekripsi, kecepatan, *sniffing* menggunakan wireshark, serta analisis *hash value* untuk memastikan integritas data. Hasil pengujian disajikan dalam bentuk grafik, tabel, dan pembahasan terstruktur untuk menjawab tujuan penelitian.
5. Bab V Kesimpulan dan Saran:

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan berdasarkan tujuan yang telah ditetapkan, serta saran untuk pengembangan sistem lebih lanjut. Kesimpulan mencakup keberhasilan implementasi sistem dan performanya dalam mengamankan data. Saran diberikan sebagai arahan bagi penelitian atau pengembangan sistem keamanan data berbasis kriptografi *post-quantum* di masa depan.