BAB 1
PENDAHULUAN

1.1 Latar Belakang

Tulisan merupakan salah satu media komunikasi yang bertujuan untuk menyampaikan pesan yang dapat mengandung suatu informasi yang bersifat rahasia. Dalam era digital, pesan dan pertukaran informasi melalui jaringan komputer menjadi kebutuhan yang tak terhindarkan. Kriptografi adalah salah satu pendekatan yang berfungsi untuk melindungi informasi baik saat proses pengiriman melalui saluran komunikasi maupun penyimpanan pada media digital (Pratiwi dkk., 2022).

Kriptografi berasal dari bahasa Yunani, yang terdiri dari kata "kryptos" yang berarti "tersembunyi" dan "graphein" yang berarti "tulisan". Sehingga kriptografi adalah menulis secara tersembunyi untuk menyampaikan pesan-pesan rahasia (Amalya dkk., 2023). Salah satu tujuan utama dari kriptografi adalah mengubah pesan asli (plainteks) menjadi pesan bersandi (cipherteks) sehingga plainteks tidak diketahui oleh pihak yang tidak diinginkan.

Terdapat dua prinsip dasar kriptografi, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Sedangkan kriptografi asimetris menggunakan sepasang kunci yang berbeda, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk melakukan enkripsi pada pesan rahasia, sementara kunci privat digunakan untuk melakukan dekripsi pada cipherteks (Saputra dkk., 2023).

Salah satu algoritma kriptografi simetris adalah Vernam *Cipher.* Penemu dari algoritma Vernam *Cipher* adalah Mayor J. Maugbome dan G. Vernam. Algoritma ini berasal dari One Time Pad *Cipher*, yang mengganti karakter dengan bit 0 atau 1. Dengan kata lain, Vernam *Cipher* adalah versi lain dari algoritma One Time Pad. Salah satu kelemahan dari algoritma One Time Pad adalah tidak mangkus karena panjang kunci sama dengan panjang pesan, sehingga akan sulit untuk melakukan proses enkripsi dan dekripsi jika pesan rahasia terlalu panjang

(Munir, 2019). Meskipun demikian, keamanan Vernam *Cipher* yang dikenal sangat kuat (secara teoritis tak terpecahkan) menjadikannya kandidat ideal untuk mengenkripsi pesan teks. Oleh karena itu, penelitian ini termotivasi untuk memanfaatkan kekuatan Vernam Cipher sebagai inti dari enkripsi pesan.

Pada penelitian oleh Silitonga (2021) membahas penerapan Vernam *Cipher* dalam penyandian pesan. Meskipun penelitian tersebut menunjukkan aplikasi praktis dari Vernam *Cipher*, ia tidak mengatasi kelemahan akan kebutuhan kunci yang harus sama panjang dengan panjang pesan.

Untuk mengatasi kelemahan panjang kunci pada Vernam *Cipher*, penelitian ini menggunakan Algoritma *Blum Blum Shub* untuk pembangkitan kunci. Algoritma *Blum Blum Shub* merupakan pembangkit bilangan acak semu yang cukup mudah dan efektif yang dibuat pada tahun 1986 oleh Lenore Blum, Manuel Blum, dan Michael Shub (Sianturi, 2020). Pemanfaatan *Blum Blum Shub* sebagai generator kunci Vernam diharapkan dapat menyediakan kunci yang panjang, acak, dan mudah dibangkitkan secara otomatis, sehingga meningkatkan efisiensi dan kepraktisan penggunaan dari Vernam *Cipher*.

Pada penelitian oleh Naufal (2021) algoritma *Blum-Blum Shub* digunakan untuk mengubah nilai pergeseran yang konstan pada *Affine Cipher* dengan bilangan acak hasil dari algoritma *Blum Blum Shub* sehingga meningkatkan keamanan pada file audio. Penelitian tersebut menunjukkan potensi penggunaan *Blum Blum Shub* dalam meningkatkan keamanan kriptografi.

Sementara itu, kelemahan lain dari kriptografi simetris adalah jika kunci enkripsi diketahui oleh pihak yang tidak berwenang, maka seluruh pesan dapat didekripsi dengan mudah. Oleh karena itu, dibutuhkan kombinasi dengan kriptografi asimetris, seperti Merkle-Hellman *Knapsack* untuk meningkatkan keamanan dalam distribusi kunci. Algoritma Merkle-Hellman *Knapsack* merupakan kriptografi asimetris awal yang ditemukan oleh Ralph Merkle dan Martin tahun 1978. Kunci yang didistribusikan pada algoritma ini adalah kunci publik, sedangkan kunci privat tidak didistribusikan. Meskipun kunci publik telah diketahui akan sulit untuk mengetahui kunci privat yang digunakan (Sari & Pawelloi, 2022). Meskipun Merkle-Hellman *Knapsack* memiliki sejarah kerentanan pada versi aslinya, prinsip dasar *Knapsack problem* yang mendasarinya

tetap menarik dan relevan untuk dieksplorasi dalam sistem hibrida. Dalam penelitian ini, Merkle-Hellman *Knapsack* dipilih untuk mengamankan distribusi kunci Vernam karena kemampuannya dalam menyediakan mekanisme kunci publik/privat yang berbeda dari algoritma asimetris lainnya, menawarkan pendekatan unik untuk masalah pertukaran kunci.

Pada penelitian oleh Aghniya (2019), algoritma Merkle-Hellman *Knapsack* digunakan sebagai kriptografi asimetris dengan kunci publik untuk enkripsi dan kunci privat untuk dekripsi kemudian dikombinasikan dengan algoritma Vigenere *Cipher* sebagai kriptografi simetris. Kedua kombinasi tersebut menghasilkan suatu kriptografi hibrida untuk membuat pesan rahasia lebih sulit untuk dipecahkan.

Perlu dilakukan pengujian untuk mengetahui kinerja dari algoritma hibrida, salah satunya dengan pengujian *Avalanche Effect* (Wardini, 2024). Pengujian ini memanfaatkan perubahan bit pada cipherteks yang diakibatkan oleh perubahan yang dilakukan terhadap plainteks maupun kunci. Semakin banyak perubahan pada bit, maka semakin baik kriptografi hibrida tersebut. Oleh karena itu, pengujian ini dapat menjadi salah satu indikator untuk menilai kekuatan kriptografi hibrida.

Pada penelitian oleh Wardini (2024), pengujian *Avalanche Effect* dilakukan pada kriptografi hibrida *Atbash, Autokey Cipher* dan El Gamal. Hasil dari penelitian tersebut menunjukkan 50% perubahan bit pada cipherteks yang diakibatkan oleh perubahan yang dilakukan pada plainteks. Sehingga kriptografi hibrida tersebut dapat dikategorikan baik karena setengah bit dari cipherteks mengalami perubahan.

Meskipun beberapa penelitian telah membahas penggunaan Vernam *Cipher* dan *Blum Blum Shub* secara terpisah, serta kombinasi Merkle-Hellman *Knapsack* dengan algoritma lain, belum ada penelitian yang menguji efektivitas kombinasi ketiga algoritma ini secara bersamaan dalam satu sistem hibrida. Dengan demikian, judul yang diambil dalam penelitian ini adalah "Implementasi Kriptografi Hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack* dalam Penyandian Pesan Teks disertai Pengujian *Avalanche Effect*". Penelitian ini mengintegrasikan keunggulan algoritma *Blum-Blum Shub* sebagai generator bilangan acak yang kuat dengan Vernam *Cipher* untuk proses enkripsi dan menggunakan Merkle-Hellman *Knapsack* sebagai mekanisme kriptografi asimetris serta pengujian *Avalanche Effect* untuk mengetahui kinerja dari kriptografi hibrida.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka dirumuskan permasalahan sebagai berikut:

1. Bagaimana rancangan pengamanan pesan teks menggunakan kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack*?
2. Bagaimana konstruksi program aplikasi pengamanan pesan teks menggunakan kriptografi kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack*?
3. Bagaimana hasil uji kriptografi hibrida Vernam *Cipher*, *Blum Blum Shub* dan Merkle-Hellman *Knapsack* menggunakan pengujian *Avalanche Effect*?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini antara lain:

1. Membuat rancangan implementasi kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack*.
2. Mengonstruksi program aplikasi kriptografi hibrida *Blum Blum Shub*-Vernam *Cipher* dan Merkle-Hellman *Knapsack*.
3. Memperoleh hasil pengujian *Avalanche Effect* pada kriptografi hibrida Vernam *Cipher*, *Blum Blum Shub* dan Merkle-Hellman *Knapsack*.

1.4 Manfaat Penelitian

Adapun manfaat penelitian ini antara lain:

1. Manfaat teoritis pada penelitian ini adalah menambah alternatif pengamanan pesan teks yang lebih aman dan kompleks, khususnya dalam kriptografi hibrida.
2. Manfaat praktis pada penelitian ini adalah untuk memudahkan pengamanan pesan menggunakan program enkripsi dan dekripsi pesan dengan kriptografi hibrida *Blum Blum Shub,* Vernam *Cipher,* dan Merkle-Hellman *Knapsack.*