BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet adalah lingkungan yang sangat tidak aman karena merupakan media komunikasi informasi yang tersimpan berupa gambar, suara, video, teks atau pesan lain. Perkembangan teknologi informasi semakin pesat terutama dalam bidang komunikasi. Seiring dengan kemajuan media sosial, isu keamanan informasi dan privasi juga menjadi aspek yang semakin penting saat ini. Hal tersebut menunjukkan bahwa keamanan dalam mentransfer data melalui internet menjadi semakin penting terutama pada keamanan informasi agar informasi yang di dapatkan tidak bisa diakses oleh orang yang tidak berhak[1].

Upaya yang di lakukan untuk meningkatkan keamanan data salah satunya dengan menerapkan teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari cara menjaga keamanan data atau pesan selama proses pengiriman, sehingga tetap terlindungi dari gangguan pihak ketiga. Salah satu metode untuk melindungi pesan dalam bentuk teks agar tidak dapat di akses oleh orang yang tidak berhak dengan mengenkripsi (*encrypt*) pesan tersebut untuk mengubahnya menjadi karakter acak yang sulit di pahami (*ciphertext*). Untuk mengembalikan pesan ke bentuk aslinya di lakukan proses deskripsi (*decrypt*) yang hanya dapat di lakukan oleh seseorang yang memiliki kunci (*key*)[2].

Kriptografi ini bertujuan untuk menjaga kerahasiaan data yang di kirim melalui suatu media, sehingga tidak dapat di akses atau di curi oleh pihak yang tidak berwenang. Terdapat berbagai metode kriptografi yang di gunakan untuk mengamankan data masing-masing dengan tingkat keamanan yang berbeda. Setiap metode memiliki kelebihan dan kekurangannya sendiri.

Namun salah satu tantangan utama dalam penggunaannya adalah menentukan algoritma kriptografi yang paling sesuai[3].

Berbagai Teknik telah diterapkan untuk melindungi data penting salah satunya adalah steganografi. Steganografi merupakan Teknik penyembunyian pesan dalam pesan lainnya sedemikian rupa sehingga keberadaannya tidak di sadari oleh orang lain. Berbeda dengan kriptografi atau metode keamanan informasi lainnya, steganografi bertujuan untuk menyisipkan informasi atau pesan ke dalam media lain seperti gambar digital, teks, audio, atau video sehingga tidak menimbulkan kecurigaan[4]. Tujuan dari steganografi adalah untuk menyembunyikan keberadaan data rahasia agar sulit di deteksi serta melindungi hak cipta suatu produk. Dalam stegnografi data yang telah di enskripsi (*ciphertext*) dapat disisipkan sedemikian rupa sehingga pihak ketiga tidak menyadari keberadaannya[5].

Sementara itu dalam steganografi pada salah satu metode yang digunakan adalah *Discrete Wavelet Transform* (DWT) yang berfungsi membagi informasi suatu sinyal menjadi bagian pendekatan yang detail. Beberapa penelitian juga telah mengombinasikan kriptografi dan steganografi guna meningkatkan keamanan pesan, sehingga pembajakan data menjadi lebih sulit karena selain harus menemukan pesan tersembunyi juga perlu mendeskripsikannya. Salah satu penelitian mengkaji kombinasi kriptografi dan steganografi berbasis *Transformasi Wavelet Diskrit Haar*, dengan citra sebagai media penampung dan teks sebagai pesan rahasia. Metode steganografi yang digunakan adalah DWT karena penelitian sebelumnya menunjukkan bahwa DWT dapat menghasilkan nilai *Peak Signal to Noise Ratio* (PSNR) yang lebih tinggi dibandingkan metode lainnya. Oleh karena itu penelitian tersebut mengusulkan kombinasi kriptografi dan steganografi berbasis *Transformasi Wavelet Diskrit* pada audio di mana teks berfungsi sebagai pesan rahasia dan audio sebagai media penyimpanan[6].

Dalam penelitian ini, dikembangkan metode keamanan data dengan mengombinasikan kriptografi dan steganografi untuk meningkatkan perlindungan informasi dalam proses transmisi data. Penelitian ini bertujuan untuk mengenkripsi pesan rahasia menggunakan teknik kriptografi, kemudian menyisipkannya ke dalam media digital dengan metode steganografi berbasis *Discrete Wavelet Transform* (DWT). Dengan pendekatan ini, pesan yang dikirimkan tidak hanya terlindungi melalui proses enkripsi tetapi juga tersembunyi dalam media tertentu, sehingga lebih sulit dideteksi dan diakses oleh pihak yang tidak berwenang[7].

Penelitian ini memilih dua algoritmanya yaitu RSA dan AES karena masing-masing memiliki keunggulan tersendiri. RSA digunakan untuk mengamankan distribusi kunci enkripsi, sementara AES digunakan untuk proses enkripsi utama karena lebih cepat dan efisien dalam menangani data dalam jumlah besar. Pendekatan ini memungkinkan sistem yang aman, efisien, dan tahan terhadap serangan, karena selain mengenkripsi data, pesan rahasia juga disisipkan dalam media menggunakan DWT, sehingga semakin sulit untuk dideteksi dan diretas.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat diidentifikasikan menjadi rumusan masalah pada penelitian ini yaitu :

1. Bagaimana menerapkan kombinasi algoritma kriptografi RSA dan AES untuk meningkatkan keamanan data dalam proses enkripsi dan dekripsi?
2. Bagaimana teknik steganografi berbasis Discrete Wavelet Transform (DWT) dapat digunakan untuk menyisipkan data rahasia ke dalam media digital agar lebih sulit dideteksi oleh pihak yang tidak berwenang?
3. Seberapa efektif metode kombinasi kriptografi RSA-AES dan steganografi berbasis DWT dalam meningkatkan keamanan dan kualitas data yang disisipkan?

1.3 Pertanyaan Penelitian

Penelitian ini bertujuan untuk mengembangkan metode keamanan data dengan mengombinasikan kriptografi dan steganografi guna meningkatkan perlindungan informasi dalam proses transmisi data. Dengan memanfaatkan algoritma RSA dan AES untuk enkripsi serta metode steganografi berbasis DWT, diharapkan pesan rahasia dapat disisipkan dalam media digital dengan aman, efisien, dan sulit dideteksi oleh pihak yang tidak berwenang.

1.4 Batasan Masalah

Berdasarkan rumusan masalah dan tujuan penelitian, maka untuk melakukan penelitian berdasarkan permasalahan yang ada, maka ditetapkan batasan masalah dalam penelitian ini sebagai berikut :

1. Penelitian ini hanya berfokus pada penyisipan teks sebagai data rahasia ke dalam media digital dalam bentuk gambar
2. Algoritma yang digunakan dalam proses enkripsi dan dekripsi adalah RSA (*Rivest-Shamir-Adleman*) dan AES (*Advanced Encryption Standard).*
3. Teknik yang digunakan untuk menyembunyikan data rahasia dalam media digital adalah *Discrete Wavelet Transform* (DWT).
4. Efektivitas metode akan diukur berdasarkan tingkat keamanan data, kualitas media setelah penyisipan, serta nilai Peak *Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE) sebagai parameter evaluasi kualitas data.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka diketahui tujuan penelitian antara lain :

1. Meningkatkan keamanan data dalam proses enkripsi dan dekripsi, penelitian ini menerapkan kombinasi algoritma RSA dan AES yang saling melengkapi dalam aspek keamanan dan efisiensi.

2. Teknik steganografi berbasis *Discrete Wavelet Transform* (DWT) digunakan dalam penelitian ini untuk menyisipkan pesan rahasia yang telah dienkripsi ke dalam media digital, seperti gambar atau audio, dengan cara membagi sinyal media menjadi beberapa sub-band frekuensi.

3. Efektivitas metode yang dikembangkan dalam penelitian ini diukur berdasarkan beberapa parameter evaluasi, seperti *Peak Signal to Noise Ratio* (PSNR) dan *Mean Square Error* (MSE) untuk menilai kualitas media setelah penyisipan pesan, serta tingkat keamanan berdasarkan analisis keberhasilan serangan terhadap data yang telah dienkripsi dan disisipkan.

1.6 Manfaat Penelitian

Berdasarkan rumusan masalah di atas, manfaat penelitian adalah sebagai berikut :

1. Menambah wawasan mengenai kombinasi teknik kriptografi dan steganografi dalam meningkatkan keamanan data digital.

2. Memberikan referensi bagi penelitian selanjutnya terkait penerapan RSA, AES, dan DWT dalam bidang keamanan informasi.

3. Memberikan solusi keamanan data yang lebih efektif, efisien, dan sulit dideteksi untuk menjaga kerahasiaan informasi dalam proses transmisi data.