BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang semakin meningkat pada era Revolusi Industri 4.0 mendorong terjadinya perubahan di berbagai aspek kehidupan. Kemajuan di bidang teknologi informasi dan komunikasi tersebut memungkinkan terjadinya pertukaran data maupun informasi menjadi semakin efektif. Namun, seiring dengan berkembangnya teknologi, terdapat juga risiko yang terjadi berkaitan dengan keamanan informasi tersebut. Risiko yang dapat terjadi seperti pencurian data, penyadapan, hingga penyebaran data maupun informasi oleh pihak lain. Dengan adanya risiko tersebut, diperlukan peningkatan keamanan guna pengamanan data dan informasi dari pihak yang tidak berwenang. Melindungi data dan informasi menjadi langkah penting yang dapat diterapkan sebagai upaya pesan atau informasi tetap aman dari pihak yang tidak berwenang (Santoso et al., 2018).

Dalam hal menjaga keamanan informasi, kriptografi merupakan salah satu aspek terpenting (Munir, 2019). Kriptografi dapat digunakan sebagai upaya untuk mengamankan data (Rakhman and Kurniawan, 2015). Kriptografi merupakan ilmu yang digunakan untuk menjaga kerahasiaan pesan atau informasi sehingga tidak dapat dipahami oleh pihak yang tidak berwenang (Santoso et al., 2018). Dengan kemampuan yang dimiliki

kriptografi dalam menjaga keamanan serta melindungi kerahasiaan menjadikan data maupun informasi yang dikirimkan dapat dipastikan keamanannya. Data dan informasi dapat disembunyikan sedemikian rupa sehinggga hanya pihak berwenang yang dapat mengaksesnya. Hal tersebut relevan dalam era saat ini, di mana dengan adanya perkembangan teknologi yang terus meningkat menjadikan pertukaran informasi terjadi dengan cepat.

Secara umum kriptografi didasarkan pada konsep-konsep matematika. Matematika menjadi dasar utama yang bersifat matematis di mana dalam algoritma kriptografi tersebut diperlukan kunci untuk melakukan proses enkripsi dan dekripsi (Munir, 2019). Pada proses enkripsi maupun dekripsi tersebut konsep-konsep yang ada dalam matematika memiliki peranan penting. Proses enkripsi dalam kriptografi merupakan suatu proses penyandian plainteks menjadi cipherteks, dan proses dekripsi merupakan proses pengembalian cipherteks menjadi plainteks awal (Munir, 2019). Konsep yang ada dalam matematika tersebut memungkinkan terciptanya pola yang terstruktur sedemikian rupa hingga menjadikan algoritma kriptografi tahan terhadap serangan guna terjaganya informasi.

Terdapat banyak algoritma kriptografi yang digunakan dalam mengamankan pesan. Algoritma kriptografi tersebut terbagi menjadi dua, yaitu algoritma kriptografi simetri dan nirsimetri. Algoritma simetri yang sering digunakan salah satunya yaitu *Vigènere Cipher* (Riadi et al., 2022). *Vigènere Cipher* merupakan algoritma yang menggunakan fungsi modulo dalam penyandiannya (Sinaga et al., 2018). Pada perkembangannya, kriptografi tidak hanya dapat diterapkan pada file teks, tetapi juga dapat digunakan pada citra digital (Sinaga et al., 2018). Contohnya penelitian Riadi et al. (2022) yang menggunakan *Vigènere Cipher* untuk melakukan enkripsi dan dekripsi citra. Penelitian tersebut mendapatkan hasil bahwa proses enkripsi dan dekripsi citra dengan Algoritma *Vigènere Cipher* dapat dilakukan dengan sangat cepat, yaitu kurang dari satu detik.

Peneliti lain, Riski et al. (2018) melakukan penelitian menggunakan

Vigènere Cipher untuk mengamankan data medis berupa citra, selanjutnya dilakukan analisis menggunakan nilai NPCR dan UACI. Nilai NPCR (*Number of Pixel Change Rate*) digunakan untuk dapat mengetahui banyaknya piksel yang berbeda dari *plain-image* (pesan berupa citra) dan *cipher-image* (pesan citra yang tersandi). Sedangkan nilai UACI (*Unified Average Changing Intensity*) digunakan untuk mengetahui besarnya interval perbedaan nilai piksel dari *plain-image* dan *cipher-image* (Wu et al., 2011).

Lebih lanjut, Vigenere Cipher memiliki kelemahan jika kuncinya pendek dan diulang secara periodik sehingga dapat ditemukan kunci berdasarkan panjang kuncinya (Munir, 2019). Oleh karena itu, beberapa peneliti menggabungkan vigenere cipher dengan algoritma lainnya untuk meningkatkan keamanan. Menggabungkan dua atau lebih metode dapat meningkatkan kerahasiaan pesan karena pesan menjadi semakin tidak mudah dipahami oleh pihak lain (Ginting, 2020). Sebagian besar sistem keamanan mengombinasikan algoritma kriptografi simetri dan nirsimetri dalam satu sistem yang dikenal sebagai *hybrid cryptosystem* (Munir, 2019). *Hybrid cryptosystem* tersebut digunakan untuk dapat meningkatkan keamanan pesan (Darari et al., 2020).

Kombinasi dari algoritma simetri dan nirsimetri memanfaatkan kelebihan dari kedua jenis algoritma kriptografi untuk mendapatkan sistem keamanan yang lebih efektif. Algoritma kriptografi simetri memiliki kelebihan dalam kecepatan proses, yaitu waktu yang relatif singkat pada proses enkripsi maupun dekripsi. Kelemahan dari kriptografi ini terletak pada aspek keamanan kunci, sehingga kunci pada kriptografi simetri harus sering diganti. Sebaliknya, kunci pada kriptografi nirsimetri tidak memerlukan penggantian kunci secara berkala, karena kriptografi ini menggunakan pasangan kunci publik dan kunci privat. Namun, proses enkripsi dan dekripsi membutuhkan waktu lebih banyak karena pada kriptografi nirsimetri digunakan bilangan bulat yang besar dan terdapatnya operasi perpangkatan (Munir, 2019).

Penelitian sebelumnya memberikan hasil bahwa kombinasi algoritma

RSA dan *Vigènere Cipher* pada citra menghasilkan enkripsi yang sulit dibaca atau dilihat secara visual (Rakhman and Kurniawan, 2015). Peneliti tersebut memberikan saran untuk menambahkan kombinasi algoritma kriptografi guna memperkuat keamanan. Penelitian tersebut sejalan dengan Darari et al. (2020) yang menunjukkan bagaimana proses *Hybrid cryptosystem* dengan algoritma RSA dan *Vigenere Cipher* untuk proses enkripsi dan deksipsi citra digital. Peneliti tersebut mendapatkan hasil enkripsi citra dengan pola yang sangat berubah dari gambar awal, sehingga cukup sulit untuk mengidentifikasi gambar aslinya (Darari et al., 2020).

Penelitian oleh Ludyawati et al. (2023) menunjukkan bahwa algoritma *Vigènere Cipher* yang dikombinasikan dengan ElGamal dapat meningkatkan keamanan suatu pesan rahasia. Lebih lanjut, peneliti lain membahas mengenai perbandingan peningkatan keamanan dengan kombinasi metode RSA, ElGamal, dan *Vigener Cipher* didapatkan bahwa banyaknya kemungkinan dipecahkannya cipherteks pada kombinasi antar masing-masing 2 metode tersebut lebih sedikit dibandingkan dengan *single* metode (Setiawan et al., 2019).

Algoritma RSA dan ElGamal merupakan algoritma kriptografi nirsimetri yang masing-masing memiliki kelebihan keamanan yang bergantung pada permasalahan matematika yang sulit dipecahkan. Algoritma RSA memiliki keunggulan pada kesulitan memfaktorkan bilangan besar menjadi faktor-faktor prima yang digunakan untuk mendapatkan kunci privat (Munir, 2019). Sementara algoritma ElGamal memiliki keunggulan yang terletak pada kompleksitas perhitungan logaritma diskrit (Hendrawaty et al., 2022).

Berdasarkan penelitian sebelumnya yang telah dilakukan, maka pada penelitian ini akan dilakukan proses enkripsi dan dekripsi citra digital dengan kombinasi *Vigènere Cipher*, Algoritma RSA, dan ElGamal beserta dengan analisis tingkat keamanan berdasarkan nilai NPCR dan UACI. Kombinasi algoritma kriptografi tersebut dilakukan untuk mendapatkan keamanan yang lebih efektif berdasarkan analisis keamanan yang

dilakukan.

1.2 Perumusan Masalah

Dengan adanya latar belakang yang ada, berikut perumusan masalah yang terdapat dari penelitian ini:

1. Bagaimana proses enkripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal?
2. Bagaimana proses dekripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal?
3. Bagaimana tingkat keamanan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal?

1.3 Batasan Masalah

Batasan masalah yang dalam penelitian ini yaitu, penelitian ini menggunakan pesan dalam bentuk citra digital.

1.4 Tujuan Penelitian

Dengan adanya permasalahan yang telah dirumuskan, tujuan dari penelitian ini yaitu sebagai berikut:

1. Melakukan proses enkripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal
2. Melakukan proses dekripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal
3. Menganalisis keamanan dari kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal

4. Melakukan perbandingan keamanan kombinasi algoritma berdasarkan hasil analisis

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang ingin dicapai, manfaat dari penelitian ini yaitu sebagai berikut:

1. Mengetahui proses enkripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal
2. Mengetahui proses dekripsi citra digital dengan kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal
3. Mengetahui perbandingan keamanan citra digital dari kombinasi algoritma *Vigènere Cipher*, algoritma RSA dan algoritma ElGamal
4. Mendapatkan kombinasi algoritma yang memiliki keamanan paling tinggi