BAB 1

PENDAHULUAN

1.1 Latar Belakang

Seiring dengan berkembangnya zaman, kemajuan wawasan ilmiah dan solusi teknologis menghasilkan inovasi yang mendukung berbagai aktivitas manusia, termasuk keterkaitan global melalui jaringan internet yang memberikan kemudahan akses informasi secara instan. Akan tetapi, situasi tersebut menghadirkan potensi ancaman siber, di mana informasi sensitif menjadi lebih rentan manipulasi oleh aktor yang tidak berwenang. Di Indonesia, tren penetrasi internet menunjukkan peningkatan yang konsisten, sebagaimana tercatat dalam oleh APJII Puspita Sari (2024). Tingkat akses internet nasional mencapai 79,5%, dengan lebih dari 221 juta penduduk yang terhubung secara aktif, naik signifikan dari 78,1% pada tahun sebelumnya. Meskipun mendorong transformasi digital, peningkatan akses ini justru memperbesar potensi celah keamanan, di mana penyerang memanfaatkan kerentanan sistem untuk mencuri atau mengubah informasi vital. Keamanan informasi, sebagai fondasi perlindungan, mencakup berbagai aspek krusial, seperti pencegahan akses oleh pihak luar, pemeliharaan kerahasiaan data pribadi, serta upaya modifikasi atau penghapusan informasi tanpa izin. Salah satu bentuk informasi yang paling sering dikirim dan berisiko tinggi adalah pesan teks.

Pesan teks telah menjadi salah satu media utama untuk pertukaran informasi sehari-hari, terutama dalam konteks komunikasi digital yang semakin mendominasi aktivitas sosial, bisnis, dan pemerintahan. Fenomena ini semakin menonjol selama pandemi COVID-19, di mana mekanisme *Work From Home* menjadi norma baru, sehingga memperbesar potensi risiko keamanan jaringan. Menurut BSSN Badan Siber dan Sandi Negara (2020), pesan teks menjadi target utama untuk penyebaran

malware. Mengingat potensi kerugian dari kebocoran rahasia bisnis atau pelanggaran privasi pribadi, keamanan dan kerahasiaan data dalam pesan teks tidak boleh diabaikan. Untuk mengatasi hal ini, diperlukan sistem keamanan pesan teks untuk menjaga kerahasiaan tersebut.

Pada peradaban awal di wilayah Mesir, Yunani, dan Romawi, orang-orang menggunakan kriptografi dalam berkomunikasi untuk merahasiakan makna dari pihak lain yang tidak mengetahuinya (Naser, 2021). Kriptografi sendiri merupakan studi matematika terkait aspek keamanan informasi (Alfred J et al., 1997). Sebelum adanya tekonologi canggih seperti zaman modern, pensil dan kertas adalah media kriptografi. Sebagian besar metode kriptografi klasik tersebut didasarkan pada pengaturan ulang alfabet atau penggantian posisi alfabet atau penggantian alfabet berbeda dari bahasa yang berbeda (Naser, 2021). Dengan kemajuan ilmu pengetahuan, teknologi kriptografi juga berkembang sangat cepat dan kebutuhan untuk menggunakan istilah baru disadari. Di era modern, dengan revolusi mesin elektronik seperti komputer, metode kriptografi bertemu dengan rumus matematika baru dengan penggunaan matematika yang luas, terdiri atas kajian teori informasi, kompleksitas komputasi, statistika, aljabar abstrak, serta disiplin matematika secara luas (Naser, 2021). Jaringan publik menjadi urgensi dalam keamanan data, di mana data akan mudah tersebar oleh pihak ketiga jika tidak diamankan (Jain, 2021).

Berdasarkan penggunaan kuncinya kriptografi dibedakan menjadi kriptografi simetris dan asimetris. Jenis kriptografi tersebut menawarkan beragam keunggulan sekaligus sejumlah kelemahan yang berpengaruh terhadap peningkatan keamanan sistem informasi (Arif and Nurokhman, 2023). Proses enkripsi dekripsi algoritma simetris bergantung pada kunci tunggal yang identik, pada algoritma asimetris diperlukan dua kunci yang berlainan untuk menjalankan kedua fungsi tersebut (Amalya et al., 2023). Untuk melindungi sistem, diperlukan suatu pendekatan yang mampu memperkuat tingkat keamanannya. Oleh sebab itu, penggabungan kedua algoritma tersebut digunakan sebagai strategi peningkatan keamanan pada pesan teks.

Meskipun kriptografi simetris memiliki keunggulan dalam kecepatan proses enkripsi dan dekripsi, metode ini kurang sesuai digunakan karena mekanisme

pengamanan kuncinya tidak cukup kuat serta kunci harus diperbarui secara berkala (Jamaludin, 2018). Sementara itu, Meskipun kriptografi asimetris menyediakan tingkat perlindungan kunci yang lebih tinggi, mekanisme enkripsi dan dekripsinya relatif kurang cepat (Suhandinata et al., 2019). Algoritma hybrid menerapkan enkripsi simetris, di mana kunci yang sama digunakan baik untuk enkripsi maupun dekripsi informasi. Sebaliknya, kriptografi berbasis kunci publik mengimplementasikan mekanisme asimetris, sehingga kunci yang berperan dalam proses dekripsi tidak serupa dengan kunci yang dipakai untuk enkripsi (Jamaludin, 2018). Algoritma asimetris menggunakan kunci enkripsi publik yang dapat diketahui oleh semua pihak, sedangkan kunci dekripsi privat hanya tersedia bagi pihak yang berhak. Oleh karena itu, integrasi antara kriptografi simetris dan asimetris diterapkan untuk mengamankan kunci simetris sekaligus meningkatkan efisiensi dan keamanan sistem informasi (Santoso, 2021). Hill Cipher merupakan salah satu metode algoritma asimetri yang akan digabungkan dengan algoritma asimetris RSA dan ElGamal.

Pada tahun 1929, Lester S. Hill memperkenalkan algoritma kriptografi klasik simetris berbasis matriks yang menggunakan operasi aljabar linear untuk enkripsi dan dekripsi pesan yang dinamankan Hill Cipher (Nur Fadlilah et al., 2022). Hill Cipher kuat dalam menghadapi serangan jika hanya dengan diketahui cipherteks saja, tetapi mudah diserang jika kriptanalis memiliki cipherteks dengan potongan plainteks kunci yang sama (Douglas R, 2006). Keamanan kunci pada Hill Cipher perlu ditingkatkan dengan melakukan penyandian terhadap kunci matriks menggunakan algoritma kriptografi asimetris seperti RSA ataupun ElGamal. RSA adalah algoritma modern asimetris yang mengandalkan kesulitan faktorisasi bilangan prima besar untuk pertukaran kunci (Putera Utama Siahaan et al., 2018). Algoritma RSA digunakan sebagai kunci publik dalam proses enkripsi pesan, sedangkan kunci privat hanya dimiliki oleh pihak tertentu dan diperlukan untuk mengembalikan pesan tersebut ke bentuk aslinya melalui proses dekripsi, begitu juga dengan ElGamal yang diperkenalkan oleh Taher ElGamal pada tahun 1985, bedanya algoritma ini berbasis pada masalah logaritma diskrit yang kesulitannya terdapat pada perhitungan modulo prima besar (Husaini et al., 2022). Meskipun demikian, algoritma keamanan hibrida yang telah dikembangkan sedemikian rupa tetap menghadapi ancaman siber yang

berkembang.

Untuk mengevaluasi keamanan kriptografi, metode serangan yang sering digunakan adalah *Brute Force Attack*. Serangan ini dianggap sebagai salah satu serangan tertua dalam seluruh sejarah keamanan siber (Verma et al., 2022). Serangan brute-force adalah serangan yang sangat dasar dan dapat digunakan terhadap setiap algoritma sandi. Dengan serangan ini, tujuannya adalah mencoba setiap kemungkinan permutasi kunci sampai menemukan kunci yang dapat menerjemahkan data menjadi teks biasa (Ayankoya and Ohwo, 2019). Artinya, jika terdapat X kunci yang berbeda, rata-rata seorang penyerang akan menemukan kunci yang sebenarnya setelah mencoba $X/2$ kali (Stallings, 2020). Kemampuan suatu skema kriptografi untuk menahan serangan menjadi indikator penting dari tingkat keamanannya, terutama dalam skenario di mana sebagian data mungkin bocor atau dapat diidentifikasi.

Dalam beberapa tahun terakhir, penelitian mengenai kombinasi algoritma kriptografi untuk meningkatkan tingkat keamanan semakin berkembang. Kombinasi algoritma simetris dan asimetris diharapkan dapat menggabungkan kecepatan dan kekuatan keamanan secara optimal. Penelitian serupa dilakukan oleh Jamaludin (2018), yang mengombinasikan Hill Cipher dan RSA dengan matriks kunci Hill 2×2. Kajian tersebut kemudian dikembangkan lebih lanjut oleh Juliana Pangaribuan (2018) serta Santoso (2021), yang memperluas ukuran menjadi 3×3 dan tetap memanfaatkan algoritma RSA. Gabungan kedua algoritma dalam sistem kriptografi hibrida dapat meningkatkan keamanan karena Hill Cipher digunakan untuk enkripsi cepat, sementara RSA mengamankan kunci yang digunakan dalam Hill Cipher.

Penelitian kedua oleh Nur Fadlilah et al. (2022) berisikan tentang ElGamal serta Hill Cipher untuk mengamankan pesan teks. Kriptografi simetris, Hill Cipher menggunakan matriks invertible sebagai kunci, dan kunci asimetris ElGamal menggunakan logaritma diskrit. Gabungan kedua algoritma tersebut untuk mengamankan pesan teks dengan cara mengonversi plaintext menjadi ciphertext menggunakan Hill Cipher, sementara ElGamal digunakan untuk mengenkripsi kunci simetris yang digunakan oleh Hill Cipher. Penelitian ini menunjukkan pesan teks teramankan dengan baik, serta dapat melindungi pesan dari serangan kriptanalis.

Penelitian ketiga dilakukan oleh Putera Utama Siahaan et al. (2018). Dalam

penelitian tersebut, dilakukan analisis perbandingan antara RSA dan ElGamal dalam hal kecepatan enkripsi dan dekripsi, serta tingkat keamanan yang ditawarkan oleh masing-masing algoritma. Hasil penelitian menunjukkan bahwa RSA memiliki kecepatan enkripsi yang lebih tinggi dibandingkan dengan ElGamal. Namun, ElGamal menunjukkan kinerja dekripsi yang lebih cepat dibandingkan RSA. Kedua algoritma ini memiliki tingkat keamanan yang tinggi, dengan RSA bergantung pada kesulitan faktorisasi bilangan bulat besar dan ElGamal bergantung pada kesulitan logaritma diskrit.

Berdasarkan penelitian terdahulu mengenai gabungan skema kombinasi kunci simetris terhadap kunci asimetris, peneliti tertarik untuk meneliti ketiga skema kombinasi. Tujuan penelitian ini untuk mengimplementasikan serta menguji kinerja dari skema yang menggabungkan (mengkombinasikan) beberapa algoritma kriptografi:

1. Hill Cipher dan RSA
2. Hill Cipher dan ElGamal
3. Hill Cipher dengan kombinasi RSA dan ElGamal

Ketiga skema sandi tersebut akan dibandingkan tingkat keamanannya, khususnya dalam menghadapi *brute force attack*. Melalui analisis perbandingan terhadap ketiga skema kombinasi algoritma tersebut, penelitian ini berupaya mengidentifikasi skema mana yang memberikan tingkat keamanan tertinggi dalam konteks keamanan sandi.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian ini adalah:

1. Bagaimana algoritma enkripsi dan dekripsi dari skema kombinasi Hill Cipher dengan RSA dan ElGamal?
2. Skema kombinasi algoritma manakah yang memberikan tingkat keamanan tertinggi terhadap Brute Force Attack?

3. Bagaimana karakteristik ukuran kunci pada algoritma yang sudah di kombinasikan agar tidak terjadi kehilangan informasi pada proses enkripsi dan dekripsi?

1.3 Batasan Masalah

Penelitian ini dibatasi untuk memperjelas ruang lingkup penelitian sebagai berikut:

1. Penelitian akan berfokus pada perbandingan empat skema kombinasi algoritma sandi berikut:
   - Sandi 1: Hill Cipher + RSA
   - Sandi 2: Hill Cipher + Elgamal
   - Sandi 3: Hill Cipher + Kombinasi (RSA dan ElGamal)
2. Penelitian ini memfokuskan penggunaan algoritma Hill Cipher dengan kunci berupa matriks berukuran 3×3.
3. Analisis utama dalam penelitian ini berfokus pada tingkat keamanan dari setiap sandi kombinasi, dengan waktu pemecahan sebagai indikator utama dalam mengukur tingkat kerentanannya.
4. Implementasi praktis dan pengujian dalam penelitian ini dilakukan dengan menggunakan kunci matriks berukuran 3×3 pada Hill Cipher sebagai objek yang diamankan melalui proses enkripsi menggunakan RSA dan ElGamal.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mendeskripsikan dan menganalisis algoritma enkripsi dan dekripsi dari skema kombinasi.
2. Membandingkan tingkat keamanan dari skema kombinasi.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Diperoleh pemahaman yang jelas mengenai mekanisme kerja dan proses matematis dari skema kombinasi tersebut.
2. Memahami bagaimana serangan tersebut dapat dilakukan dan faktor-faktor yang mempengaruhi keberhasilannya.
3. Menentukan skema mana yang memberikan tingkat keamanan tertinggi terhadap *brute force attack*.