BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan cabang matematika yang memiliki peran dalam mengatasi kebocoran sistem informasi dan komunikasi pada pengiriman dan penerimaan pesan. Hal itu dikarenakan kriptografi dapat menjaga kerasahasiaan pesan dengan menyembunyikan pesan asli yang dirubah menjadi sandi yang kemudian dikirim kepada penerima, sehingga pesan sulit untuk disadap oleh seseorang yang tak memiliki wewenang. Pada ilmu kriptografi pesan asli disebut *Plaintext*, sementara pesan yang sudah disandikan merupakan *Ciphertext*. Dalam pengaplikasiannya, terdapat 2 proses utama (*Enkripsi* dan *Dekripsi*) yang ada pada kriptografi. Proses menyandikan plainteks menjadi cipherteks disebut Enkripsi, sedangkan proses mengembalikan cipherteks menjadi plainteks semula disebut Dekripsi [1].

Kriptografi menggunakan kunci sebagai langkah-langkah penyandian pesan dari plainteks menjadi cipherteks, yang mana kunci tersebut nantinya akan diberikan atau ditukar oleh pengirim kepada penerima pesan. Berdasarkan kunci yang telah dipakai untuk enkripsi dan dekripsi, algoritma kunci kriptografi dapat dikelompokan menjadi tiga yaitu, algoritma simetri, asimetri, dan fungsi hash. Algoritma simetri merupakan algoritma kriptografi yang hanya memiliki satu kunci, atau memiliki kunci yang sama, sedangkan algoritma asimetri merupakan algoritma kriptografi yang memiliki dua kunci, yaitu kunci pribadi (*private key*) dan kunci publik (*public key*) [1], [2].

Perkembangan kriptografi semakin pesat seiring dengan perkembangan teknologi dalam kehidupan manusia. Hal ini bisa dilihat dari banyaknya subjek-subjek pembelajaran yang ada pada kriptografi. Kegunaan algoritma-algoritma kunci yang muncul dari banyaknya reformasi pada peperangan dunia, baik itu ke-1

dan ke-2, menjadikan kriptografi sebagai teknik terpenting dalam keamanan informasi khususnya komunikasi. Sebagai contoh algoritma-algoritma kriptografi yang sudah lahir yaitu Hill Cipher, Vegenere Cipher, Multiplicative Cipher, Caesar Cipher yang termasuk ke dalam algoritma simetri, kemudian juga ada RSA (*Rivest, Shamir, Adleman*), DES (*Data Encryprion Standard*), blowfish yang termasuk ke dalam algoritma asimetri [1].

Kriptografi secara kategori bisa dikelompokan ke dalam 2 jenis, yaitu *Classical Cryptography* (klasik) dan *Modern Cryptography* (modern). Algoritma Vigenere dan Hill cipher termasuk ke dalam *Classical Cryptography* dimana pada pengimplementasiannya, kedua algoritma tersebut menggunakan teknik substitusi. Pada sebuah penelitian *International Conference on Intelligent Systems and Computer Vision* tahun 2020 yang berjudul "*Text Encryption: Hybrid Cryptographic Method Using Vigenere and Hill Ciphers*" membahas terkait pengkombinasian dua algoritma yang nantinya berfokus pada proses enkripsi dan dekripsinya. Penelitian tersebut bertujuan untuk mengatasi kekebalan kunci algoritma Vigenere cipher yang mudah diserang oleh seorang kriptanalis menggunakan metode *kasiski*. Dikarenakan panjang kuncinya yang rentan dibaca, sehingga dibutuhkan kombinasi dengan Hill cipher yang sama-sama menggunakan teknik substitusi [3].

Algoritma Hill cipher merupakan algoritma kriptografi yang menggunakan matriks transformasi dalam proses enkripsi dan dekripsi pesan. Hill cipher ini dapat mengubah sebuah pesan menjadi suatu blok matriks yang nantinya akan dienkripsi menggunakan kunci matriks, sehingga hasilnya dapat meminimalisir kesamaan kunci dalam setiap huruf pada pesan plainteks [1]. Hal inilah yang membuat metode ini sangat sulit diserang oleh kriptanalisis sehingga algoritma Vigenere Cipher akan kebal terhadap serangan dengan metode kasiski. Akan tetapi masih terdapat masalah pada metode Hill cipher, yang mana dapat diserang dengan metode *Known Plainteks-Attack*. Sehingga pada jurnal yang berjudul "*A New Approach of Classical Hill Cipher in Publik Cryptography*" ditulis oleh Rajaa K. Hasouna, Sameerah Faris Khalebusa, Huda Kadhim Tayyeha [4], membahas tentang kekurangan yang ada pada algoritma kunci simetri yang hanya memiliki satu kunci,

yaitu pada Hill cipher, sehingga perlu ditingkatkan dengan algoritma asimetri yang memiliki kunci publik, yaitu algoritma RSA (Rivesh, Shamir, Adleman).

Algoritma RSA merupakan algoritma kunci publik yang tingkat keamanannya jauh lebih tinggi dibanding algoritma kunci publik lain. Sulitnya memfaktorkan bilangan bulat besar menjadi faktor-faktor primanya merupakan salah satu keunggulan yang dimiliki oleh RSA. Sehingga algoritma RSA dapat membantu meningkatkan kekurangan yang ada pada algoritma Hill Cipher. Akan tetapi, meski keamanan pada kombinasi Hill Cipher dengan RSA meningkat, proses untuk membangkitkan kuncinya membutuhkan tahapan dan langkah yang rumit untuk enkripsi dan dekripsi pesan, Sehingga dalam jurnal tersebut perlu adanya pembangkit kunci yang dapat dengan efisien lebih memudahkan proses algoritma. Salah satu pembangkit kunci yang digunakan adalah dengan matriks involusi.

Selain itu pembangkit kunci pada RSA, khususnya pada kunci publik, saat ini sudah mulai bisa terpecahkan oleh seorang penyadap menggunakan metode Faktorisasi Fermat, dengan mencari nilai n hasil kali dari 2 buah bilangan prima. Karena kunci pribadi sangat berhubungan dengan kunci publik, penemuan metode ini cukup menguntungkan pihak penyadap untuk melemahkan keamaanan pada algoritma RSA. Sehingga dibutuhkan pembangkit kunci lain untuk menguatkan keamanan kuncinya, salah satunya dengan metode *Enhanced and secured RSA key generation scheme* (ESRKGS) [12]. Metode tersebut mengandalkan 4 buah bilangan prima yang dibangkitkan untuk mempersulit pemecahan pada kunci publik.

Berdasarkan latar belakang diatas yang juga didukung 2 penelitian sebelumnya oleh para peneliti. Penulis berharap dapat melakukan suatu percobaan penelitian yang menggabungkan 2 konsep algoritma pada penelitian tersebut. Sehingga penulis dapat mengkaji pembahasan ini lebih lanjut dengan mengangkat judul pada penelitian ini yaitu **"Algoritma *Hybrid* : Vigenere-Hill Cipher dan RSA (Rivest, Shamir, Adleman) dengan pembangkit kunci matriks involusi".**

1.2 Rumusan Masalah

Adapun Rumusan Masalah yang akan dikaji dalam tugas akhir ini merujuk pada latar belakang di atas yaitu :

1. Bagaimana proses modifikasi Algoritma *Hybrid* Vigenere-Hill Cipher dan RSA (Rivest, Shamir, Adleman) dengan pembangkit kunci involusi dan ESRKGS?
2. Bagaimana proses enkripsi dan dekripsi Algoritma *Hybrid* Vigenere-Hill Cipher dan RSA (Rivest, Shamir, Adleman) dengan pembangkit kunci involusi dan ESRKGS?
3. Bagaimana simulasi pengiriman pesan menggunakan algoritma *hybrid*?

1.3 Batasan Masalah

Dalam pembahasan masalah tersebut, terdapat beberapa batasan yang harus diperhatikan antara lain adalah:

1. Pengkodean yang digunakan adalah karakter ASCII dalam rentang modulo 256.
2. Matriks yang digunakan sebagai kunci pada pembangkit kunci matriks involusi adalah *Invertible Matriks*, yaitu matriks yang berbentuk persegi dan berdeterminan tak nol.
3. Panjang kunci yang digunakan pada proses enkripsi dan dekripsi pesan menggunakan vigenere cipher itu sepanjang 4 karakter.
4. Proses enskripsi dan dekripsi pesan per 16 karakter.

1.4 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah disebutkan, tujuan dari penelitian ini adalah untuk :

1. Untuk mengetahui proses modifikasi Algoritma *Hybrid* Vigenere-Hill Cipher dan RSA (Rivest, Shamir, Adleman) dengan pembangkit kunci involusi dan ESRKGS.
2. Untuk mengetahui proses enkripsi dan dekripsi Algoritma *Hybrid* Vigenere-Hill Cipher dan RSA (Rivest, Shamir, Adleman) dengan pembangkit kunci involusi dan ESRKGS.
3. Untuk Mengetahui Bagaimana Simulasi pengiriman pesan menggunakan algoritma *hybrid*.

1.5 Metodologi

1. Studi Literatur

   Pada langkah ini, identifikasi permasalahan dilakukan dengan mencari referensi yang mendukung tugas akhir dan berkaitan dengan algoritma kriptografi. Referensi ini dapat diperoleh dari berbagai sumber seperti buku, jurnal, paper, dan artikel terkait.

2. Analisis

   Pada tahap ini algoritma yang telah direpresentasikan akan dicari celah untuk proses kombinasinya sehingga didapatkan suatu linieritas dari tiap-tiap algoritmanya.

3. Simulasi

   Pada tahap ini dilakukan simulasi enkripsi dan dekripsi pesan untuk menunjukan bagaimana proses algoritma *Hybrid*, baik dalam modifikasi algoritma, pengiriman dan pengamanan pesan.

4. Kesimpulan

   Pada tahap ini diperoleh kesimpulan dari kombinasi algoritma yang dapat dijadikan suatu algoritma baru serta hasil dari simulasi.

1.6 Sistematika Penulisan

Berdasarkan sistematika penulisannya, penelitian ini terdiri dari lima bab, daftar pustaka serta lampiran.

BAB I PENDAHULUAN

Pada bagian ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang berkaitan dengan permasalahan yang dikaji dalam penelitian ini. Secara umum teori yang dipaparkan mencakup definisi Teori bilangan, matriks serta sifat-sifatnya, Kriptografi secara umum, Algoritma Vigenere Cipher, Algoritma Hill Cipher, dan RSA standar serta improvisasi.

BAB III MODIFIKASI ALGORITMA VIGENERE-HILL CIPHER DAN RSA DENGAN PEMBANGKIT KUNCI MATRIKS INVOLUSI DAN ESRKGS

Bab ini berisi penjelasan utama mengenai proses pemodifikasian Algoritma simetri dan asimetri menjadi Agoritma *Hybrid* Vigenere-Hill Cipher dan RSA dengan pembangkit kunci matriks involusi dan ESRKGS serta proses enkripsi dan dekripsinya.

BAB IV SIMULASI PENGIRIM PESAN MENGGUNAKAN ALGORITMA *HYBRID*

Bab ini akan dijelaskan mengenai simulasi pengiriman pesan, enkripsi dan dekripsi, menggunakan algoritma hybrid.

BAB V PENUTUP

Bagian terakhir penulisan ini adalah bab penutup yang bersisi kesimpulan atas semua pembahasan serta saran untuk pengembangan topik pembahasan penelitian ini.