BAB 1
PENDAHULUAN

1.1 Latar Belakang Penelitian

Teknologi dan informasi saat ini berkembang semakin pesat, sehingga proses pertukaran data dan informasi dapat dilakukan dengan sangat mudah melalui berbagai macam media (Kusumaningsih et al, 2017). Namun, perkembangan teknologi ini juga menyebabkan banyaknya cara untuk menyadap suatu informasi. Oleh karena itu, keamanan data sangatlah penting guna mencegah kebocoran dan penyalahgunaan data dengan tidak semestinya oleh pihak-pihak yang tidak bertanggung jawab. Hal ini dikarenakan beberapa informasi hanya ditujukan untuk sekelompok orang tertentu.

Salah satu ilmu yang mempelajari kemanan data adalah kriptografi, di mana ilmu ini mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Menezes, 1996). Kriptografi dapat pula diartikan sebagai ilmu untuk menjaga keamanan pesan. Ketika data tersebut dikirim dari satu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak yang tidak seharusnya. Untuk menjaga kerahasiaan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti oleh pihak lain (Amin, 2016).

Salah satu metode kriptografi yang digunakan untuk menjaga kerahasiaan informasi adalah enkripsi dan dekripsi (Reswan dan Prabowo, 2018). Enkripsi merupakan proses pengubahan pesan menjadi sandi, sedangkan dekripsi merupakan proses pengubahan sandi menjadi pesan semula. Enkripsi dan dekripsi ini dapaat menggunakan kriptografi simetris maupun kriptografi asimetris. Kriptografi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Sedangkan, kriptografi asimetris menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya.

Algoritma El Gamal merupakan salah satu kriptografi asimetris yang pertama kali ditemukan oleh Taher El Gamal pada tahun 1985. Keamanan dari algoritma ini didasarkan pada sulitnya memecahkan logaritma diskrit pada penggandaan bilangan bulat modula prima yang besar (Ifanto, 2009).

Vigènere *cipher* adalah salah satu kriptografi klasik yang pertama kali dipublikasikan oleh seorang diplomat dan kriptologis asal Perancis, Blaise de Vigènere pada tahun 1586. Sedangkan, algoritma *autokey* Vigènere *cipher* merupakan Vigènere cipher ketika panjang kunci lebih pendek daripada panjang plainteks, kekurangan tersebut akan ditambahkan dengan plainteksnya (Munir 2019).

Penelitian mengenai kriptografi Vigènere *cipher* dan algoritma El Gamal ini sudah banyak, salah satu penelitiannya yaitu yang dilakukan oleh Firdaus pada tahun 2017 dengan judul "Penyandian Pesan Menggunakan Kombinasi Algoritma RSA yang Ditingkatkan dan Algoritma El Gamal". Penelitian tersebut menggabungkan algoritma RSA yang ditingkatkan dengan algoritma El Gamal, di mana kedua algoritmanya termasuk ke dalam kriptografi asimetris. Selain itu, ada pula penelitian yang dilakukan oleh Pratiwi pada tahun 2014 dengan judul "Program Aplikasi Kriptografi Penyandian *One Time Pad* Menggunakan Sandi Vigenere". Penelitian tersebut menggabungkan algoritma Vigènere *cipher* dan *one* time pad.

Pada tahun 2018, Ariska, Suroso dan Endri melakukan penelitian dengan judul "Rancangan Kriptografi Hybrid Kombinasi Metode Vigènere Cipher dan Elgamal pada Pengamanan Pesan Rahasia". Penelitian ini menggabungkan kriptografi Vigènere *Cipher* dengan algoritma El Gamal. Algoritma Vigènere *cipher* ini memiliki kelemahan, yaitu ketika panjang kunci lebih pendek daripada panjang plainteksnya, maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteksnya. Kelemahan ini memudahkan pengkriptanalisisan pesan dengan menggunakan metode Kasiski untuk mengetahui panjang kunci dan frekuensi analisis untuk mengetahui kata kunci (Munir, 2004). Sehingga, penulis tertarik untuk meneliti bentuk lain dari Vigènere *Cipher* yaitu algoritma *autokey* Vigènere *Cipher*. Algoritma *autokey* Vigènere *cipher* ini dianggap lebih aman dibandingkan algoritma Vigènere *cipher* karena akan meminimalisir kelemahan dari Vigènere *cipher* biasa (*Full Vigènere cipher*). Hal ini telah diteliti oleh Safei pada tahun 2012 dengan judul "Pengukuran dan Pengujian Kekuatan Algoritma Auto-key Vigènere *Cipher*".

Bagaimanapun kriptografi simetris memiliki kelemahan yaitu pada

pendistribusian kunci karena enkripsi dan dekripsi menggunakan kunci yang sama (Madhira dan Samulal, 2014). Demi meningkatkan keamanan pesan rahasia, penulis tertarik menggunakan teknik kriptografi *hybrid*, yaitu menggabungkan kriptografi simetris dan kriptografi asimetris. Kriptografi *hybrid* memiliki performa yang lebih baik dan kerahasiaan pesan dapat dicapai dengan pendekatan kriptografi *hybrid* (Francis dan Monoth, 2018). Selain itu, Basri pada tahun 2015 menyebutkan bahwa implementasi metode *hybrid* memiliki tingkat keamanan yang lebih baik dibanding hanya menggunakan metode kriptografi simetris ataupun hanya kriptografi asimetris.

Dengan demikian, penulis mengkaji penelitian dengan judul "Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey* Vigènere *Cipher* dan Algoritma El Gamal".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah dibahas sebelumnya, maka penulis merumuskan masalah penelitian sebagai berikut :

a. Bagaimana prosedur penyandian pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal?
b. Bagaimana konstruksi program aplikasi penyandian pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal?

1.3 Batasan Masalah

Dirumuskan batasan masalahnya adalah sebagai berikut:

a. Data yang akan disandikan berupa pesan teks.
b. Algoritma pada enkripsi dan dekripsi pesan menggunakan algoritma *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal.
c. Pembangkitan kunci pada algoritma El Gamal dibangkitkan secara acak.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk:

a. Menyandikan pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal.
b. Mengimplementasikan penyandian pesan dengan menggunakan kriptografi *hybrid autokey* Vigènere *cipher* dan algoritma El Gamal pada sebuah program aplikasi.

1.5 Manfaat Penelitian

Manfaat dilakukannya penelitian ini adalah sebagai berikut :

a. Manfaat teoritisnya yaitu diharapkan penelitian ini dapat memberikan landasan bagi para peneliti dalam melakukan pengembangan penelitian dengan menggunakan kriptografi *hybrid* guna menyandikan pesan.
b. Manfaat praktisnya yaitu diharapkan penelitian ini dapat digunakan sebagai metode baru dalam penyandian pesan menggunakan kriptografi *hybrid* dan memudahkan pengguna dalam menyandikan menggunakan program aplikasi.

1.6 Sistematika Penulisan

Secara garis besar sistematika pembahasan dalam penelitian ini sebagai berikut :

BAB I: PENDAHULUAN

Berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II: LANDASAN TEORI

Berisi tentang teori-teori penunjang yang akan digunakan dalam bab selanjutnya, meliputi teori dasar kriptografi, Vigènere *cipher*, *autokey* Vigènere *cipher*, Algoritma El Gamal, Kriptografi *hybrid* dan landasan matematika yang mendasari kriptografi dalam penelitian ini.

BAB III: METODE PENELITIAN

Berisi tentang proses atau cara ilmiah yang akan digunakan dalam penelitian ini.

BAB IV: HASIL DAN PEMBAHASAN

Membahas penyandian pesan dengan menggunakan kriptografi *hybrid auto-key* Vigènere *cipher* dan algoritma El Gamal beserta implementasinya pada sebuah program.

BAB V: PENUTUP

Berisi tentang simpulan dan saran yang dieroleh dari pembahasan yang telah dilakukan.