BAB I
PENDAHULUAN

1.1 Latar Belakang

Tulisan adalah salah satu media dalam berkomunikasi yang juga bertujuan menyampaikan pesan yang berada di dalam tulisan yang mungkin mengandung informasi bersifat rahasia. Di era digital isu keamanan data menjadi salah satu isu pokok. Adapun informasi yang bersifat rahasia tentu harus terjaga keamanannya. Kriptografi adalah salah satu ilmu yang berbasis pada keamanan data, dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan juga autentikasi (Simbolon dkk., 2020).

Kata "kriptografi" sendiri berasal dari bahasa Yunani, yaitu "*crypto"* dan "*graphia"*. "*Crypto"* yang berarti "*secret"* dan diterjemahkan menjadi "rahasia", serta "*graphia"* yang berarti "*writing"* dan diterjemahkan menjadi "tulisan". Kriptografi juga merupakan ilmu dan seni yang berguna untuk menyamarkan isi suatu pesan (informasi) yang dimaksudkan untuk menjaga kerahasiaan saat pesan dikirim dari satu pihak kepihak yang lain (Munir, 2006).

Kriptografi memuat beberapa istilah yang di antaranya adalah plainteks, enkripsi, cipherteks dan dekripsi. Enkripsi merupakan proses yang terjadi pada saat penyandian pesan dari pesan asli yang dapat dimengerti (plainteks) hingga menjadi suatu pesan tersamar yang tidak dapat dimengerti dengan mudah (cipherteks). Sementara dekripsi merupakan proses kebalikannya yaitu proses yang terjadi pada saat mengubah atau mengembalikan cipherteks menjadi plainteks. Di mana pada proses enkripsi dan dekripsi tersebut akan memerlukan suatu algoritma atau kunci tertentu (Firdaus dkk., 2018).

Kriptografi dapat dibagi menjadi dua kategori, yaitu kriptografi simetri dan asimetri. Pada kriptografi simetri sendiri memakai kunci yang sama untuk melakukan proses enkripsi dan dekripsinya. Sementara kriptografi asimetri memakai kunci yang berbeda untuk melakukan proses enkripsi dan dekripsinya (Atika, 2018).

Salah satu kriptografi asimetri yaitu algoritma El Gamal yang ditemukan oleh Taher El Gamal pada tahun 1985. Algoritma El Gamal menitikberatkan persoalan

keamanan pada sukarnya pemecahan dalam masalah logaritma diskrit khususnya pada penggandaan bilangan bulat modulo prima yang besar (Husaini dkk., 2022).

Salah satu kriptografi simetri yaitu ada Vigènere *cipher* yang disebarluaskan oleh Blaise de Vigènere di tahun 1586 guna menyandikan plainteks menggunakan teknik substitusi. Pada metode Vigènere *cipher*, terdapat variasi kunci *autokey cipher*. *Autokey cipher* adalah Vigènere *cipher* yang menggunakan kunci yang lebih pendek dari pesan aslinya. Selanjutnya *atbash cipher* adalah *cipher* substitusi monoalfabetik dengan memetakan setiap huruf ke kebalikannya, sehingga huruf pertama menjadi huruf terakhir, huruf kedua menjadi huruf kedua terakhir, dan seterusnya.

Akan tetapi pada kriptografi simetri terdapat kelemahan dalam pendistribusian kunci dikarenakan penggunaan kunci yang sama untuk proses enkripsi maupun dekripsinya (Mandangan dkk., 2016). Untuk menambahkan keamanan pesan yang berisi informasi yang bersifat rahasia, maka akan digunakan teknik kriptografi *hybrid* yang merupakan gabungan dari kriptografi simetri dengan kriptografi asimetri. Dengan pendekatan melalui kriptografi *hybrid*, maka kerahasiaan informasi dari suatu pesan dapat dicapai karena kriptografi *hybrid* juga akan memberikan performa yang lebih baik (Dewi dkk., 2022). Selain itu, disebutkan bahwa penerapan metode *hybrid* mempunyai tingkat keamanan yang lebih baik apabila dibandingkan dengan memakai metode kriptografi simetri saja atau kriptografi asimetri saja (Basri, 2015).

Untuk mengetahui kinerja dari algoritma *hybrid*, perlu dilakukan pengujian keamanan. Pengujian tingkat keamanan dapat dilakukan dengan pengujian *Avalanche Effect* (AE) (Ramanujam & Karuppiah, 2011). Pengujian *Avalanche Effect* (AE) sebagai salah satu alat ukur keamanan kriptografi di mana pengujian *Avalanche Effect* (AE) memanfaatkan perubahan bit yang terjadi dalam cipherteks, yang diakibatkan oleh perubahan yang dilakukan terhadap plainteks maupun kunci (Fadlan, 2021). Dalam pengujian *avalanche effect*, semakin banyak perubahan bit maka semakin baik model tersebut. Uji *avalanche effect* dapat dikategorikan baik apabila setengah bit dari cipherteks mengalami perubahan.

Penelitian yang berkaitan dengan pengujian *avalanche effect*, kriptografi *atbash*-a*utokey cipher* dan algoritma El Gamal ini sebelumnya juga ada beberapa,

salah satunya yakni yang dilakukan oleh Fadlan (2021) yang mengangkat judul "Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data". Di dalam penelitian ini menggabungkan antara *autokey cipher* dengan algoritma *atbash* untuk proses enkripsi dan dekripsinya sehingga menghasilkan kesimpulan yang menunjukkan bahwa algoritma kriptografi *atbash cipher* yang dipadukan dengan algoritma *autokey cipher*, mampu menghasilkan pesan tersandi yang lebih sulit untuk dipecahkan daripada pesan yang tersandi hanya dengan *autokey cipher*.

Ada pula Hikmah (2020) dengan penelitian yang berjudul "Penyandian Pesan dengan Menggunakan Kriptografi *Hybrid Autokey* Vigènere *cipher* dan Algoritma El Gamal". Penelitian tersebut menggabungkan antara *autokey cipher* dengan algoritma El Gamal untuk proses enkripsi dan dekripsinya. Diketahui bahwa algoritma Vigènere *cipher* mempunyai kelemahan, yakni apabila panjang kunci lebih pendek dari pesan aslinya, maka kunci harus diulang hingga panjang karakter pada kunci sama dengan karakter pada pesan aslinya. Kelemahan ini tentunya sangat mempermudah pengkriptanalisis pesan, yang mana dengan hanya memakai teknik Kasiski untuk dapat langsung memperoleh panjang kunci serta frekuensi analisis untuk mengetahui kata kunci (Munir, 2006). Oleh karena itu, penelitian ini akan membahas tentang *atbash* dan *autokey cipher*. Algoritma ini dipandang lebih baik dalam tingkat keamanannya dibanding dengan hanya menggunakan Vigènere *cipher* biasa atau hanya dengan *autokey cipher*.

Selanjutnya pada penelitian yang dilakukan oleh Fadlan (2021), dengan judul "Pengujian Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom". Berdasarkan penelitian tersebut, metode yang hanya menggunakan *autokey cipher* mendapatkan hasil rata-rata nilai *Avalanche Effect* sebesar 1,66% yang artinya tingkat keamanan pada *autokey* masih termasuk dalam kategori lemah.

Berdasarkan penjelasan yang telah disebutkan, maka penulis tertarik untuk melakukan penelitian dengan judul "Kriptografi *Hybrid Atbash-Autokey Cipher*, dan Algoritma El Gamal dalam Pengamanan Pesan dan Pengujian *Avalanche Effect* (AE)".

1.2 Rumusan Masalah

Penelitian ini memiliki rumusan masalah sebagai berikut:

1. Bagaimana rancangan kriptografi *hybrid* antara *atbash* c*ipher*, *autokey* c*ipher*, dan algoritma El Gamal dalam pengamanan pesan?
2. Bagaimana mengkonstruksi program aplikasi dalam penyandian pesan menggunakan kriptografi *hybrid* antara *atbash* c*ipher*, *autokey* c*ipher*, algoritma El Gamal?
3. Bagaimana hasil uji kriptografi *hybrid* antara *atbash* c*ipher*, *autokey* c*ipher*, algoritma El Gamal menggunakan pengujian *avalanche effect* ?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Menerapkan kriptosistem baru hasil kombinasi antara *atbash* c*ipher*, *autokey* c*ipher*, dan algoritma El Gamal dalam penyandian pesan.
2. Membuat program aplikasi sederhana kombinasi antara *atbash* c*ipher*, *autokey* c*ipher*, dan algoritma El Gamal.
3. Memperoleh hasil pengujian *avalanche effect* pada kriptografi *hybrid* antara *atbash* c*ipher*, *autokey* c*ipher*, algoritma El Gamal.

1.4 Manfaat Penelitian

Penelitian ini memiliki manfaat sebagai berikut:

1. Manfaat Teoritis

   Penelitian ini menggambarkan rancangan kriptografi *hybrid* dalam menjaga kerahasiaan pesan dengan kriptosistem kombinasi antara *atbash-autokey* c*ipher*-algoritma El Gamal serta pengujian keamanannya dengan *avalanche effect* (AE). Diharapkan dapat menjadi dasar atau tumpuan kepada peneliti selanjutnya dalam melakukan pengembangan penelitian menggunakan kriptografi *hybrid*.
2. Manfaat Praktis

   Penelitian ini akan menghasilkan sebuah program aplikasi GUI Python yang *user-friendly* untuk yang dapat digunakan untuk menyamarkan pesan menggunakan kriptografi *hybrid* dan menguji keamanan pesan tersamar menggunakan *avalanche effect* (AE).