BAB I

PENDAHULUAN

1.1 Latar Belakang

Tulisan merupakan salah satu cara berkomunikasi. Untuk merahasiakan isi tulisan (pesan) tersebut, kita dapat memanfaatkan suatu metode yang disebut kriptografi. Pada perkembangan digital dalam pertukaran informasi saat ini, kriptografi m asih menjadi metode yang digunakan untuk merahasiakan suatu informasi (pesan). Kriptografi adalah ilmu dan seni yang menyamarkan isi suatu pesan (informasi) untuk menjaga keamanan dan kerahasiaannya ketika pesan dikirim dari satu pihak ke pihak yang lain (Munir, 2006).

Kriptografi dapat terbagi menjadi dua jenis yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris adalah teknik kriptografi yang menggunakan satu kunci yang sama pada proses enkripsi dan dekripsi. Sedangkan Kriptografi asimetris adalah teknik kriptografi yang menggunakan kunci yang berbeda pada proses enkripsi dan dekripsinya.

Mesin Enigma adalah sebuah mesin pengenkripsi pesan yang digunakan oleh Militer Jerman pada saat Perang Dunia II (Nugroho, 2013). Mesin Enigma termasuk ke dalam kriptografi simetris karena menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Prinsip dasar kerja mesin Enigma adalah dengan melakukan substitusi huruf beberapa kali melalui rotor-rotor, *reflector,* dan beberapa komponen mesin lainnya. Tingkat keamanan mesin Enigma dapat dihitung dari jumlah kemungkinan posisi awal pengaturan rotor-rotor yang ada pada mesin. Diperkirakan ada sekitar 15.000.000.000.000.000.000 kombinasi yang mungkin terjadi jika sebanyak 3 rotor digunakan pada mesin (Lingga, 2019). Hal ini menyebabkan mesin Enigma dianggap sebagai alat kriptografi yang canggih dan mustahil untuk dipecahkan pada saat itu.

Dalam proses pengiriman dengan mesin Enigma, *cipher text* dikirimkan bersamaan dengan kunci berupa pengaturan awal mesin. Kunci ini digunakan oleh penerima pesan untuk melakukan pendekripsian pesan karena Enigma termasuk kriptografi simetri sehingga pada proses pendekripisian dibutuhkan kunci yang sama dengan proses pengenkripsian.

Athala Dwi Cahyani, 2022
PENYAMARAN TEKS DENGAN SKEMA HYBRID MENGGUNAKAN ALGORITMA ENIGMA DAN ALGORITMA ELGAMAL
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

Pada masa PD II, pihak militer Polandia (yang saat itu perang dengan Jerman) menugaskan seorang matematikawan bernama Marian Rejewski dari Poznan University untuk melakukan kriptanalisis terhadap Enigma (Christensen, 2007). Rejewski memanfaatkan teori permutasi dan grup *cycle* untuk menentukan pengaturan awal rotor pada mesin Enigma dan pengaturan pasangan huruf pada rotornya serta memperhatikan kelemahan Enigma yang sudah ada, seperti huruf asli (*plain text*) tidak bisa dienkripsi menjadi huruf yang sama. Awalnya kinerja Rejewski dinilai cukup karena sudah bisa memecahkan beberapa huruf yang sudah dienkripsi dengan mesin Enigma, hingga akhirnya pihak Militer Jerman mengubah *reflector* Enigma dan memberikan peraturan pengaturan awal rotor yang berbeda setiap harinya dalam internal militer. Pada saat itu metode yang dipakai Rejewski dinilai tidak lagi efisien untuk mendekripsi pesan *cipher* Enigma.

Kemudian seorang matematikawan asal Inggris, Alan Turing, menciptakan sebuah mesin elektromekanik bernama *The Bombe* untuk mengidentifikasi urutan posisi dan pengaturan rotor (Welchman, 1997). Berangkat dari penemuan Rejewski sebelumnya, *The Bombe* dapat mendeteksi bahwa saat terjadi kontradiksi saat proses pengidentifikasian kemungkinan pengaturan awal mesin, maka lanjutkan ke kemungkinan selanjutnya. Ketika terjadi kontradiksi, sebagian besar pengaturan yang mungkin akan dibuang sehingga menyisakan sedikit kemungkinan lain untuk diperiksa. Kontradiksi terjadi ketika huruf *cipher* yang didekripsi kembali menjadi huruf *plain text* dengan huruf yang sama, yang tidak mungkin terjadi pada penyandian Enigma.

Berangkat dari penemuan Alan Turing yang dapat mendeteksi kontradiksi saat mengidentifikasi kemungkinan pengaturan awal mesin (dalam hal ini kunci simetris), sebagai upaya untuk melindungi kunci Enigma dari pihak asing, dapat dilakukan pengenkripsian kunci Enigma dengan menggunakan kriptografi asimetris. Pada penelitian sebelumnya, Prasetio, Triandi, & Hardianto (2018) menggunakan algoritma RSA untuk mengenkripsi kunci pesan yang dienkripsi oleh Enigma. Selain itu algoritma ElGamal sebagai salah satu kriptografi asimetris juga digunakan pada kriptografi hybrid dengan kriptografi *Autokey* Vigenere *Cipher* yang merupakan kriptografi simetris oleh Hikmah (2018).

Pada penelitian ini akan digunakan algoritma ElGamal untuk mengenkripsi kunci pesan Enigma. Algoritma ElGamal dipilih karena sulitnya menyelesaikan masalah algoritma diskrit akibat bilangan acak k yang dipilih pada saat proses enkripsi dirahasiakan (Firdaus, Marwati, & Gozali, 2018), sehingga algoritma ElGamal dianggap aman untuk mengamankan kunci pesan Enigma yang berisi pengaturan awal mesin.

Pada penelitian ini akan dirancang suatu aplikasi pengamanan file teks dengan menggunakan skema *hybrid* algoritma Enigma dan algoritma ElGamal. Algoritma Enigma digunakan untuk menyamarkan informasi pesan yang akan dienkripsi, sementara algoritma ElGamal digunakan untuk menyamarkan kunci pesan yang telah dienkripsi. Perbedaan penelitian ini dengan penelitian sebelumnya adalah pilihan reflektor yang digunakan. Pada penelitian sebelumnya pengguna tidak dapat memilih reflektor yang ingin digunakan, aplikasi yang dibuat hanya menggunakan satu reflektor yaitu reflektor B. Pada penelitian ini pengguna dapat memilih satu dari tiga rotor yang ada. Aplikasi dirancang untuk mempermudah pengguna dalam memilih rotor awal yang akan digunakan. Aplikasi yang dirancang dibuat menggunakan bahasa pemrograman Python.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dikemukakan, rumusan masalah yang akan dibahas dalam proposal penelitian ini adalah

1) Bagaimana skema untuk menyamarkan teks dengan metode *hybrid* menggunakan algoritma Enigma dan algoritma ElGamal.
2) Bagaimana konstruksi program aplikasi menyamarkan teks dengan metode *hybrid* menggunakan algoritma Enigma dan algoritma ElGamal dengan Python.

1.3 Tujuan Penelitian

Tujuan penelitian ini adalah:

1) Untuk membuat skema menyamarkan file teks menggunakan metode *hybrid* dengan algoritma Enigma dan ElGamal.

2) Untuk membuat konstruksi program menyamarkan file teks menggunakan metode *hybrid* dengan algoritma Enigma dan ElGamal dengan bahasa pemrograman Python.

1.4 Batasan Masalah

Yang menjadi batasan masalah dalam proposal skripsi antara lain:

1) Karakter yang digunakan pada algoritma Enigma adalah 26 huruf alphabet.
2) Menyediakan lima buah rotor dari seluruh delapan buah rotor yang ada pada mesin Enigma.
3) Karakter yang digunakan pada algoritma ElGamal menggunakan tabel ASCII 128.
4) Bahasa yang digunakan untuk mengkonstruksi program adalah Python.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini antara lain:

1) Manfaat Teoritis

   Penelitian ini menggambarkan rancangan konstruksi model program sebagai alternatif kriptografi *hybrid* dalam menjaga kerahasiaan pesan dengan algoritma Enigma dan ElGamal. Harapannya model yang dibuat dapat dikembangkan oleh peneliti lain di waktu yang akan datang.

2) Manfaat Praktis

   Program aplikasi yang dibuat dengan pemrograman Python dapat digunakan untuk menyamarkan pesan teks dan kuncinya dengan algoritma Enigma dan ElGamal agar terjaga kerahasiaannya.