BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi dan informasi dari masa ke masa terus mengalami perkembangan yang sangat pesat dan berpengaruh pada hampir semua aspek kehidupan manusia, salah satunya adalah bidang komunikasi. Komunikasi adalah salah satu cara untuk saling bertukar informasi. Kemajuan teknologi memudahkan orang untuk mengakses informasi. Namun seiring berkembangnya teknologi seringkali pesan yang dikirim diretas oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena itu diperlukan adanya suatu sistem yang dapat digunakan untnuk mengamankan informasi tersebut. Media informasi yang digunakan pada saat ini ada berbagai jenis. Jenis-jenis media yang sering di antaranya berupa berupa teks, gambar, video atau audio.

Kriptografi berasal dari bahasa Yunani: *cryptos* dan *graphein*. *Cryptos* artinya rahasia, sedangkan *graphein* artinya tulisan. Jadi, kriptografi berarti tulisan rahasia. Sedangkan definisi kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Schneier, 1996). Kriptografi bisa membuat data yang akan dikirimkan diamankan terlebih dahulu untuk menjaga kerahasiaan data. Pesan yang dirahasiakan dinamakan *plaintext*, sedangkan pesan hasil penyandian disebut *ciphertext*. Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi dan proses membalikkan *ciphertext* menjadi *plaintext* disebut dekripsi. Proses enkripsi dan dekripsi pada sistem kriprografi memerlukan kunci.

Kriptografi diklasifikasikan menjadi dua jenis berdasarkan kuncinya, kunci simetris dan kunci asimetris (Chandra dkk, 2014). Sistem kriptografi kunci simetri menggunakan satu kunci yang sama untuk melakukan enkripsi dan dekripsi. Kriptografi kunci simetris memberikan waktu enkripsi dan dekripsi yang cepat. Metode pertukaran kunci dengan aman dibutuhkan pada kriptografi kunci simetris karena kunci yang digunakan pada proses enkripsi dan dekripsi sama. Contoh dari algoritma kunci simetri adalah AES, DES, *Blowfish*.

Kriptografi kunci asimetris menggunakan kunci publik dari penerima pesan untuk proses enkripsi dan penerima pesan menggunakan kunci privat untuk dekripsi pesan yang diamankan (Chandra dkk, 2014). Contoh dari algoritma kriptografi kunci asimetris adalah RSA, ECC, dan DSA.

Algoritma *Blowfish* diciptakan oleh Schneier di *Cambridge Security Workshop* pada Desember 1993 untuk menggantikan algoritma DES (Schneier, 2005). Algoritma *Blowfish* telah dianalisis secara luas dan diterima sebagai algoritma enkripsi yang baik. Beberapa keunggulan algoritma *Blowfish* adalah kesesuaian dan efisiensinya untuk mengimplementasikan pada perangkat keras dengan beban komputasi rendah. Algoritma *Blowfish* juga tidak dipatenkan dan oleh karena itu tidak memerlukan lisensi apapun untuk menggunakannya (Alabaichi, 2013).

Algoritma *Blowfish* adalah algoritma enkripsi simetris yang menggunakan kunci rahasia yang sama untuk proses enkripsi maupun dekripsi (Khatri, 2014). Algoritma *Blowfish* termasuk *block cipher*, *block cipher* merupakan teknik dalam kriptografi modern yang bekerja dengan cara membagi *plaintext* menjadi beberapa *block bit*, yang kemudian dienkripsi menggunakan kunci menjadi *block-block bit ciphertext* menurut Fauzi dkk (2021). Algoritma *Blowfish* membagi pesan menjadi *block* yang panjangnya ditentukan saat enkripsi dan dekripsi. Panjang dari *block* untuk *Blowfish* adalah 64 *bit*.

Kelebihan dari Algoritma *Blowfish* adalah ringkas dan dapat dijalankan dengan kapasitas memori rendah. Algoritma *Blowfish* tidak dipatenkan sehingga dapat digunakan secara bebas oleh setiap orang dalam situasi apapun (Khatri, 2014). Algoritma *Blowfish* adalah simplifikasi dari prinsip yang digunakan di DES sehingga memberikan keamanan yang serupa, lebih efisien dan lebih cepat dibanding DES (Alabaichi, 2013).

Kriptografi visual adalah tipe dari skema kriptografi yang berfokus pada penyelesaian masalah penyembunyian pesan di dalam gambar. Kriptografi visual awalnya dikemukakan oleh Moni Naor dan Adi Shamir pada tahun 1994 di konferensi Eurocrypt (Weir, 2011). Ketika beberapa *share* dari gambar yang telah terenkripsi ditumpuk, *plain* gambar akan terbentuk dengan sedikit *noise*. Proses penumpukan beberapa *share* gambar tersebut tidak diperlukan adanya proses komputasi apapun.

Sebelumnya terdapat beberapa peneliti yang mengkaji tentang kriptografi visual, yaitu Zahra dkk (2021) menggunakan algoritma *Elliptic Curve Cryptography* untuk melakukan kriptografi pada gambar berwarna. Pada penelitian tersebut pengamanan gambar dilakukan dengan mengkonversi warna dasar *Red, Green, Blue* (*RGB*) menjadi *shared image* yang sulit dikenali. Lalu pada penelitian berikutnya oleh Rakhman dkk (2015) melakukan kriptografi pada gambar *bitmap* 8 *bit* menggunakan algoritma RSA dan *Vigenere Cipher*. Pada penelitian tersebut dilakukan konversi nilai *Red, Green, Blue* pada setiap *pixel* di gambar sehingga gambar yang terenkripsi sulit dikenali.

Algoritma *Blowfish* telah dianalisis secara luas dan diterima sebagai algoritma enkripsi yang kuat dengan beberapa keunggulan seperti kesesuaian dan efisiensi saat diimplementasikan. Algoritma *Blowfish* memberikan tingkat keamanan serupa dengan DES namun lebih efisien dan lebih cepat dibandingkan DES (Alabaichi, 2013). Pada penelitian yang dilakukan oleh Thakur dkk (2011) melakukan analisis kinerja terhadap DES, AES, dan *Blowfish*, didapatkan hasil yaitu kinerja *Blowfish* lebih baik dibandingkan kedua algoritma lainnya.

Beberapa penelitian tentang algoritma *Blowfish* di antaranya yaitu Abdullah dkk (2016) melakukan implementasi algoritma *Blowfish* dan metode *Least Significant Bit Insertion* pada video Mp4. Pada penelitian tersebut dilakukan proses kriptografi pada teks menggunakan algoritma *Blowfish*, lalu menyisipkan pesan terenkripsi ke dalam *bit* tertentu dari *file* video Mp4 menggunakan metode *Least Significant Bit*. Penelitian berikutnya oleh Yuliana (2014) melakukan implementasi algoritma kriptografi *Blowfish* dan metode steganografi *End of File* (*EOF*) untuk keamanan data. Pada penelitian tersebut pesan asli akan dilakukan enkripsi oleh algoritma *Blowfish* lalu dilakukan steganografi ke suatu gambar menggunakan metode *End of File*. Penelitian berikutnya oleh Zuli dkk (2016) melakukan implementasi kriptografi dengan algoritma *Blowfish* dan Riverst Shamir Adleman (RSA) untuk proteksi *file*. Penelitian tersebut mengamankan *file* menggunakan algoritma *Blowfish* terlebih dahulu lalu dienkripsi lagi menggunakan RSA, menghasilkan *file* yang sudah diamankan oleh dua algoritma tersebut.

Pada penelitian ini akan dilakukan konstruksi program kriptografi pada media gambar menggunakan algoritma *Blowfish*. Hasil penelitian ini diharapkan dapat memberikan pemahaman

dan referensi untuk melakukan penelitian lebih lanjut mengenai implementasi Algoritma *Blowfish* pada citra lain selain gambar maupun citra gambar.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah pada penelitian ini adalah:

1. Bagaimana implementasi algoritma *Blowfish* secara teoretis pada kriptografi gambar?
2. Bagaimana konstruksi program aplikasi kriptografi gambar menggunakan algoritma *Blowfish*?

1.3 Batasan Masalah

Batasan masalah yang akan digunakan pada penulisan ini adalah format gambar yang digunakan berupa PNG.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang diuraikan, maka tujuan dari penelitian ini adalah:

1. Mengetahui implementasi algoritma *Blowfish* secara teoretis pada kriptografi gambar.
2. Membuat program aplikasi kriptografi gambar menggunakan algoritma *Blowfish*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Memudahkan pengguna dalam enkripsi dan dekripsi gambar menggunakan program aplikasi.
2. Memberikan kontribusi pada bidang matematika terapan serta menambah referensi mengenai algoritma *Blowfish* pada kriptografi gambar.