BAB I
PENDAHULUAN

1.1. Latar Belakang

Di era *modern* ini, dunia digital memiliki peran penting dalam kehidupan sehari-hari. Salah satunya dalam pertukaran informasi. Beberapa dekade lalu, jika hendak berkomunikasi dan mengirimkan pesan diperlukan media berupa surat yang kemudian dikirimkan melalui pos. Saat ini dengan berkembangnya teknologi, bertukar pesan bisa dilakukan tanpa perlu keluar rumah dengan menggunakan jaringan internet. Selain dapat mengirimkan pesan, internet juga bisa menjadi sarana dalam mengirimkan file multimedia, salah satunya adalah file video. Menurut Siswanto dkk. (2015) video merupakan serangkaian gambar atau *frame* yang ditampilkan pada layar dengan kecepatan tertentu sehingga rangkaian *frame* tampak "bergerak". Selain menampilkan rangkaian *frame*, video juga menyimpan data audio.

Mengirimkan file video melalui jaringan internet bisa saja berisiko dikarenakan orang asing bisa dengan mudah mengakses file yang diunggah pada jaringan internet. Sehingga keamanan file yang akan dikirim harus terjamin, khususnya jika file tersebut sangat rahasia. Oleh karena itu, perlu adanya suatu solusi untuk mengamankan file video yang akan dikirimkan melalui jaringan internet agar pihak lain tidak dapat mengetahui isi video yang akan dikirimkan.

Ilmu atau seni untuk menjaga keamanan pesan dengan cara menyandikannya sehingga isi dari pesan tersebut tersamarkan dan tidak memiliki makna disebut kriptografi (Munir, 2010). Di dalam kriptografi terdapat dua proses yang dijalankan. Proses untuk menyamarkan suatu pesan atau gambar asli disebut sebagai proses enkripsi. Proses untuk mengembalikan suatu pesan atau gambar yang telah disamarkan ke bentuk aslinya disebut sebagai proses dekripsi. Terdapat sebuah "kunci" untuk melakukan proses enkripsi dan proses dekripsi (Qadir & Varol, 2019). Selain untuk menyandikan pesan, kriptografi dapat digunakan untuk menyamarkan media lain seperti gambar, audio dan video.

Berdasarkan algoritma kriptografi terdapat dua jenis algoritma yang umum digunakan, yaitu algoritma kriptografi simetris dan algoritma kriptografi asimetris.

Algoritma kriptografi simetris memiliki kunci enkripsi dan kunci dekripsi yang sama, sedangkan algoritma kriptografi asimetris memiliki kunci enkripsi dan kunci dekripsi yang berbeda. Algoritma kriptografi simetris memiliki kelemahan di mana pengirim dan juga penerima pesan harus memiliki kunci yang sama, sehingga perlu adanya suatu mekanisme untuk meningkatkan keamanan algoritma kriptografi simetris. Mekanisme yang bisa digunakan antara lain memodifikasi algoritma kriptografi simetris atau membuat sebuah skema pengiriman kunci kriptografi dengan cara yang aman (Munir, 2010).

Salah satu teknik yang digunakan untuk menyamarkan video adalah teknik transposisi. Transposisi dilakukan untuk mengacak urutan *frame* atau *pixel* pada video dan mengacak urutan data audio sehingga tampilan dan suara dari file video dapat tersamarkan. (Zalukhu, 2018) melakukan penelitian untuk mengacak tampilan video dengan menggunakan algoritma transposisi zigzag dan menghasilkan tampilan video yang sulit dikenali. Selain itu, Jawahir dan Haviluddin (2015) menggunakan teknik transposisi untuk menyamarkan file audio. Kedua penelitian tersebut berhasil menerapkan teknik transposisi untuk menyamarkan isi video dan audio. Tetapi, perlu adanya penggabungan dengan algoritma kriptografi lainnya untuk memberikan *noise* dan meningkatkan tingkat keamanan file video.

Algoritma kriptografi klasik yang umum digunakan untuk mengamankan pesan adalah algoritma *Affine Cipher*. Algoritma *Affine Cipher* merupakan algoritma kriptografi simetris klasik yang dimanfaatkan untuk enkripsi pesan huruf, di mana setiap huruf akan dikonversi menjadi urutan angka lalu dengan memanfaatkan perhitungan matematika sederhana akan menghasilkan urutan huruf yang teracak (Mezaal & Abdulkareem, 2017). Algoritma kriptografi klasik memiliki tingkat keamanan yang rendah dikarenakan algoritma kriptografi klasik memiliki proses perhitungan kunci yang lebih sederhana dibandingkan dengan algoritma kriptografi modern. Salah satu teknik untuk meningkatkan keamanan algoritma *Affine Cipher* adalah dengan memodifikasi algoritma tersebut menjadi algoritma *Random Matrix Affine Cipher (RMAC)*. Video terdiri dari kumpulan *frame* di mana setiap *frame*-nya memiliki nilai *pixel* yang kemudian dienkripsi. *Random Matrix Affine Cipher* mengenkripsi setiap nilai *pixel* yang ada di setiap

baris dan kolom yang ganjil dan genap dengan menggunakan parameter kunci yang berbeda-beda. Sehingga, nilai setiap *pixel* pada baris dan kolom yang berbeda akan menghasilkan nilai cipher *pixel* yang berbeda (Lone dkk., 2021). Secara kasat mata hasil dari enkripsi menggunakan algoritma *Affine Cipher* sudah bisa memberikan *noise* pada tampilan video. Pada penelitian ini akan dilihat bagaimana perbedaan hasil keteracakan *pixel* dari algoritma *Affine Cipher* asli dibandingkan dengan algoritma *Random Matrix Affine Cipher* dengan menggunakan analisis nilai korelasi, diagram *scatter plot* dan banyaknya kemungkinan kunci kriptografi.

Penelitian lainnya yang menerapkan teknik transposisi atau algoritma *Affine Cipher* untuk kriptografi file video antara lain penelitian yang dilakukan oleh Agrawal dkk. (2018) untuk mengamankan file video menggunakan teknik transposisi permutasi zigzag dan algoritma *AES*. Pada penelitian tersebut file video dipisahkan menjadi kumpulan *frame*. Lalu urutan setiap *frame* diacak menggunakan algoritma transposisi zigzag. Kemudian, setiap *frame* yang telah teracak dienkripsi menggunakan algoritma kriptografi *AES* dan diubah kembali menjadi video. Hasil dari penelitian tersebut menghasilkan cipher video yang sulit untuk dikenali. Lalu pada penelitian yang dilakukan oleh Mishra dkk. (2015) file video diamankan menggunakan algoritma *Matrix Affine Cipher* dan *Two Dimensional Discrete Wavelet Transform* sehingga dapat menghasilkan file video tersamarkan. Untuk mengamankan data audio, Naufal (2021) melakukan penelitian kriptografi audio menggunakan transposisi dan *Affine Cipher* yang dikembangkan dengan algoritma *Blum Blum Shub*. Teknik transposisi berhasil menyamarkan file audio sehingga tersamarkan, tetapi memerlukan algoritma enkripsi untuk meningkatkan keamanannya. Hasil dari penelitian tersebut, algoritma modifikasi *Affine Cipher* yang digunakan berhasil meningkatkan keamanan file audio dan juga memberikan *noise* pada data audio sehingga sulit untuk dikenali.

Berdasarkan pemaparan di atas, penulis tertarik untuk mengimplementasikan penggabungan transposisi dan algoritma kriptografi *Random Matrix Affine Cipher* untuk melakukan kriptografi pada file video. Diharapkan hasil penelitian ini dapat memberikan pengetahuan mengenai kriptografi pada file video dengan menggunakan penggabungan transposisi dan algoritma *Random Matrix Affine Cipher* serta dapat menghasilkan sebuah aplikasi

untuk menjalankan proses kriptografi pada file video dari mulai proses pembangkitan kunci, proses enkripsi dan proses dekripsi.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah pada penelitian ini sebagai berikut:

1. Bagaimana proses kriptografi pada video dengan transposisi dan algoritma *Random Matrix Affine Cipher*?
2. Bagaimana peningkatan keamanan dari *Affine Cipher* asli dibandingkan dengan *Random Matrix Affine Cipher* pada video?
3. Bagaimana konstruksi program aplikasi kriptografi video dengan transposisi dan algoritma *Random Matrix Affine Cipher*?

1.3. Batasan Masalah

Dikarenakan keterbatasan kemampuan perangkat yang digunakan pada penelitian ini, maka batasan masalah yang digunakan pada penelitian ini adalah:

1. File video yang digunakan memiliki resolusi maksimal 240p.
2. File video yang digunakan memiliki kecepatan *frame* 30 *fps*.
3. File video yang digunakan menggunakan jenis audio mono 16-bit.
4. Format file video yang digunakan adalah format *.avi yang memiliki sifat *uncompressed video format*.

1.4. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan pada penelitian ini sebagai berikut:

1. Mengimplementasikan enkripsi file video dengan transposisi dan algoritma *Random Matrix Affine Cipher*.
2. Menganalisis peningkatan keamanan dari *Affine Cipher* asli menjadi *Random Matrix Affine Cipher* pada video.
3. Mengkonstruksi program aplikasi kriptografi video dengan transposisi dan algoritma *Random Matrix Affine Cipher*.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Manfaat Teoritis

   Secara teoritis penelitian ini bermanfaat dalam memberikan pengetahuan mengenai bagaimana pengamanan file video menggunakan transposisi dan *Random Matrix Affine Cipher*.

2. Manfaat Praktis

   Secara praktis penelitian ini menghasilkan program aplikasi menggunakan bahasa pemrograman *Python* mengenai pengamanan file video menggunakan transposisi dan algoritma *Random Matrix Affine Cipher* yang diharapkan dapat digunakan dan dimanfaatkan oleh *user*.

1.6. Sistematika Penulisan

Sistematika penulisan penelitian ini sebagai berikut:

1. **BAB I PENDAHULUAN**

   Bab ini menjelaskan mengenai latar belakang penelitian, rumusan masalah, tujuan penelitian dan manfaat penelitian.

2. **BAB II KAJIAN TEORI**

   Bab ini mengandung teori dasar matematika dan konsep-konsep mengenai transposisi dan algoritma kriptografi yang dikaji dari beberapa sumber literatur yang menunjang penelitian.

3. **BAB III METODOLOGI PENELITIAN**

   Bab ini menjelaskan mengenai model dasar dan langkah-langkah yang digunakan dalam menyelesaikan penelitian.

4. **BAB IV HASIL DAN PEMBAHASAN**

   Bab ini membahas mengenai hasil penelitian yang telah dilakukan dan menjelaskan konstruksi program yang telah dibuat.

5. **BAB V KESIMPULAN DAN SARAN**

   Bab ini memberikan kesimpulan hasil penelitian dan saran-saran untuk penelitian selanjutnya.