

BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

Informasi kini menjadi sebuah kunci utama dalam segala hal. Pada masa lampau, penguasa dunia adalah dia yang memiliki pasukan yang banyak. Adanya teknologi membuat pasukan yang banyak tak lagi menguasai dunia. Pada era sekarang ini penguasa dunia adalah dia yang menguasai informasi. Barang siapa yang dapat menguasai semua informasi, maka ia dapat menguasai dunia.

Dikarenakan pentingnya informasi, berbagai cara digunakan untuk mengamankan informasi yang dimiliki agar tidak jatuh pada pihak yang tidak memiliki hak untuk mengetahui informasi tersebut. Informasi dalam bentuk teks dapat disandikan menjadi informasi lain yang tidak jelas dengan teknik kriptografi. Kriptografi merupakan ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentifikasi data (Wahana Komputer, 2010).

Salah satu algoritma kriptografi klasik adalah *Caesar cipher*, yang mana algoritma ini bekerja dengan menggeser tiga abjad ke kanan untuk setiap karakter pada deret huruf alfabet. Algoritma ini digunakan pada zaman romawi untuk menyandikan pesan yang akan disampaikan kepada sekutunya.

Semakin canggih teknologi informasi, semakin rentan keamanan sebuah informasi, oleh karenanya diperlukan penemuan atau perbaikan algoritma yang ada. Pada algoritma *caesar cipher*, pergeseran huruf dilakukan dengan jumlah pergeseran yang sama pada setiap karakter. Pada tugas akhir ini penulis akan mengembangkan algoritma *caesar cipher* dengan pergeseran yang berbeda-beda pada setiap karakter yang diinputkan dengan memanfaatkan nilai intensitas warna pada citra digital.

Setiap orang yang pernah menggunakan sandi rahasia berupa teks pada teknik kriptografi, kemungkinan besar mereka pernah mengalami lupa dengan sandi yang dibuat, sehingga ciphertext tidak dapat diterjemahkan. Dari kasus ini penulis akan membuat sebuah sandi berupa gambar digital sebagai sandi dalam proses enkripsi dan dekripsi. Dengan demikian, pengguna akan lebih mudah mengingat sandi yang digunakan dalam bentuk gambar.

Setiap piksel pada citra RGB 24-bit memiliki nilai intensitas *red*, *green*, *blue* yang masing-masing berkisar dari 0 s/d 255, nilai inilah yang akan dijadikan nilai pergeseran pada

masing-masing karakter dalam teks yang akan dienkripsi. Citra digital yang telah diinputkan akan diubah resolusinya menjadi 100 x 100 piksel untuk mendapatkan pola pergeseran yang lebih beragam. Nilai intensitas warna akan dibaca dan akan dideretkan untuk setiap piksel pada citra digital dalam bentuk data teks.

Untuk memberikan keamanan yang lebih kuat, pengguna dapat menentukan index awal pada data teks intensitas warna yang telah dibuat. Dengan demikian, untuk dapat mendekripsikan kembali *ciphertext*, pengguna harus memiliki citra digital yang dipakai untuk enkripsi dan index yang ditentukan saat proses enkripsi.

Berdasarkan paparan di atas maka algoritma *caesar cipher* dapat dikembangkan dengan pergeseran yang berbeda pada setiap karakternya. Sehingga tugas akhir ini berjudul **Teknik Kriptografi untuk Menjaga Keamanan Informasi dengan Memanfaatkan Citra Digital sebagai Kunci.**

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan permasalahan yang akan diselesaikan dalam penelitian ini adalah:

1. Bagaimana mengimplementasikan algoritma *caesar cipher* yang telah dikembangkan pergeseran karakternya pada text file?
2. Bagaimana mengimplementasikan citra berwarna sebagai kunci untuk enkripsi dan dekripsi?

1.3 Batasan Masalah/Ruang Lingkup

Adapun batasan masalah/ruang lingkup masalah dalam penelitian ini sebagai berikut:

1. Aplikasi menggunakan bahasa pemrograman java dengan Netbeans IDE.
2. Informasi yang disandikan dalam bentuk teks.
3. Kunci untuk proses enkripsi dan deskripsi adalah citra digital RGB 24-bit (ukuran 100 x 100 piksel)

1.4 Tujuan

Berdasarkan rumusan masalah tersebut maka tujuan dari penelitian ini adalah:

1. Mengembangkan algoritma *caesar cipher* dalam pergeseran karakter.
2. Membangun aplikasi kriptografi dengan algoritma yang telah dikembangkan dengan menggunakan citra digital sebagai kuncinya.

1.5 Manfaat

Manfaat yang diharapkan dengan terbangunnya aplikasi kriptografi ini adalah:

1. Mengamankan data dalam bentuk teks.
2. Memudahkan seseorang untuk mengingat kunci saat enkripsi atau dekripsi.