BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi informasi, informasi menjadi sangat mudah untuk didapatkan. Irwansyah dan Moniaga (2004) mengemukakan bahwa, “Teknologi Informasi adalah pengertian umum untuk berbagai jenis teknologi tersedia dengan tujuan membantu manusia untuk menjalani hidup dengan lebih mudah dan lebih baik dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi”. Perkembangan teknologi informasi membawa banyak manfaat terhadap berbagai bidang, khususnya dalam hal penyampaian informasi. Di balik manfaat tersebut, keamanan dan kerahasiaan dari informasi yang bertebaran harus diperhatikan. Tanpa adanya keamanan informasi, pencurian informasi oleh pihak berwenang dapat terjadi sewaktu-waktu. Oleh karena itu, keamanan informasi menjadi hal yang harus ditingkatkan sesuai dengan perkembangan teknologi.

Nurul, dkk. (2022) mengemukakan bahwa "Keamanan informasi didefinisikan sebagai melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kemudahan penggunaan.". Salah satu cara dalam mengamankan informasi adalah menggunakan kriptografi. Menezes, dkk. (2001) mengemukakan bahwa “Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi”. Dengan menggunakan kriptografi, keamanan dari suatu informasi dapat ditingkatkan melalui proses enkripsi dan dekripsi. Kriptografi dapat diterapkan pada berkas dengan jenis teks, gambar, audio, maupun video.

Affine Cipher merupakan algoritma kriptografi yang termasuk ke dalam algoritma kriptografi klasik. Munir (2019) mengemukakan bahwa *Affine Cipher* bukanlah algoritma yang aman karena sepasang kuncinya (m dan b) dapat ditemukan dengan *exhaustive key search* (*brute force attack*). Naufal (2021) mengemukakan bahwa keamanan *Affine Cipher* dapat ditingkatkan dengan

menggunakan barisan bilangan acak. Penggunaan barisan bilangan acak sebagai kunci *Affine Cipher* memungkinkan enkripsi suatu nilai yang sama menghasilkan nilai enkripsi yang berbeda.

Cryptographically secure pseudorandom number generator (*CSPRNG*) adalah pembangkit bilangan acak yang aman digunakan untuk kriptografi. Munir (2019) mengemukakan bahwa sebuah *CSPRNG* memiliki dua syarat untuk dipenuhi yaitu mempunyai sifat-sifat yang bagus secara statistik dan tahan terhadap serangan yang serius dalam memprediksi bilangan acak yang dihasilkan. Terdapat beberapa *CSPRNG* di antaranya yaitu *Blum Blum Shub*, *CSPRNG* berbasis RSA, *CSPRNG* berbasis *Chaos*, dsb. *CSPRNG* berbasis *Chaos* memiliki properti yang berharga dalam kriptografi yaitu peka terhadap perubahan nilai awal. *CSPRNG* berbasis *Chaos* membangkitkan bilangan acak menggunakan fungsi *chaos*, yang mana salah satunya yaitu fungsi logistik.

Penelitian yang dilakukan oleh Zelvian (2023) membahas implementasi kriptografi gambar menggunakan algoritma *Blowfish*. Penelitian tersebut hanya menggunakan satu kunci untuk mengenkripsi setiap nilai piksel pada gambar. Hasil enkripsi dari piksel-piksel berdekatan yang memiliki nilai sama menghasilkan nilai yang sama juga, hal ini mengakibatkan terbentuknya suatu objek dari hasil tersebut. Sama halnya dengan menggunakan sepasang kunci saja pada algoritma *Affine Cipher* akan menghasilkan gambar hasil enkripsi yang kurang baik, sehingga penggunaan pembangkit bilangan acak sebagai kunci-kunci pada *Affine Cipher* diharapkan dapat menghasilkan gambar hasil enkripsi yang lebih baik. Selain itu, penelitian yang dilakukan oleh Naufal (2021), memanfaatkan algoritma pembangkit bilangan acak *Blum Blum Shub* untuk meningkatkan keamanan *Affine Cipher*.

Penelitian ini membahas konstruksi implementasi kriptografi gambar dengan menggunakan algoritma *Affine Cipher* dengan pembangkit bilangan acak *CSPRNG* berbasis *Chaos*. Oleh karena itu, penelitian ini mengambil judul **"Kriptografi Gambar Menggunakan Algoritma *Affine Cipher* dan *Cryptographically Secure Pseudorandom Number Generator* Berbasis *Chaos*"**.

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang tersebut, permasalahan dapat dirumuskan sebagai berikut:

1) Bagaimana skema algoritma *Affine Cipher* dan *CSPRNG* berbasis *Chaos* pada kriptografi gambar?
2) Bagaimana konstruksi program aplikasi kriptografi gambar dengan menggunakan algoritma *Affine Cipher* dan *CSPRNG* berbasis *Chaos*?
3) Bagaimana peningkatan kualitas enkripsi gambar dari algoritma *Affine Cipher* dengan menggunakan *CSPRNG* berbasis *Chaos*?

1.3 Batasan Masalah

Batasan masalah yang akan digunakan dalam penelitian ini adalah gambar aras keabuan (*grayscale*) dengan kedalaman 8 bit dan gambar berwarna (RGB) dengan kedalaman 8 bit pada setiap kanalnya dengan format JPEG, JPG, atau PNG.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan penelitian ini adalah:

1) Mengetahui implementasi algoritma *Affine Cipher* dan *CSPRNG* berbasis *Chaos* pada kriptografi gambar.
2) Membuat program aplikasi kriptografi gambar menggunakan algoritma *Affine Cipher* dan *CSPRNG* berbasis *Chaos.*
3) Mengetahui peningkatan kualitas enkripsi gambar dari algoritma *Affine Cipher* dengan menggunakan *CSPRNG* berbasis *Chaos.*

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1) Memberikan alternatif kriptografi pada gambar dengan menggunakan *Affine Cipher* dan *CSPRNG* berbasis *Chaos*
2) Menyediakan program aplikasi untuk pengaman pesan gambar dengan *Affine Cipher* dan *CSPRNG* berbasis *Chaos.*