# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Berkembang pesatnya teknologi komunikasi dan informasi memberikan beberapa pengaruh negatif berupa ancaman keamanan komunikasi melalui jaringan internet. Ancaman-ancaman tersebut bisa berupa interupsi, penyadapan, modifikasi maupun fabrikasi. Dengan berkembangnya ilmu pengetahuan, penerapan teknik pengamanan informasi yang sudah dipakai sejak dahulu bisa menjadi alternatif dalam pengamanan komunikasi data melalui jaringan internet, sebagai contoh adalah kriptografi.

Dalam penerapannya, kriptografi disebut dengan istilah enkripsi. Selain kriptografi, steganografi menjadi salah satu alternatif pengamanan dalam komunikasi data. Melalui penelitian ini penulis mengkombinasikan kedua teknik pengamanan informasi dengan merancang dan mengimplementasikan sistem steganografi berbasis SSB-4 dengan enkripsi *text secret message* menggunakan algoritma *Cipher Hill* yang dimodifikasi.

Algoritma *Cipher Hill* adalah salah satu algoritma kriptografi kunci simetris yang merupakan penerapan aritmatika modulo pada kriptografi, dan termasuk kedalam kategori cipher blok. Dasar teori matriks yang digunakan dalam *Cipher Hill* yang dimodifikasi antara lain adalah perkalian antar matriks dan melakukan *invers* dengan memanfaatkan *pseudoinvers* pada matriks berukuran *m x n.*

Setelah proses enkripsi dilakukan dengan menggunakan metode *Cipher Hill* yang dimodifikasi, dilanjutkan dengan melakukan proses penyisipan bit menggunakan metode SSB-4. Metode SSB-4 adalah teknik penggantian bit ke-4. Tiap bit dari karakter *ciphertext* akan disisipkan pada bit ke-4 di setiap *pixel* pada *Cover-Image*. Perancangan kombinasi dua metode tersebut dapat diterapkan pada pengiriman pesan melalui jaringan internet *via e-mail* sehingga data bisa lebih terjamin kerahasiaannya.

## 1.2. Tujuan

1. Memahami metode *Cipher Hill* secara umum.
2. Mendesain sistem steganografi berbasis SSB-4 pada citra digital.
3. Melakukan enkripsi terhadap *text secret message* dengan algoritma *Cipher Hill* yang dimodifikasi dan mengkombinasikan dengan skema SSB-4.
4. Mengimplementasikan kombinasi sistem tersebut pada perangkat lunak Matlab.
5. Menganalisa performansi (*time process* dan *robustness*).
6. Menganalisa kualitas output yang dihasilkan dengan parameter MOS (*Most Opinion Score*), MAE (*Mean Absolute Error*), MSE (*Mean Squared Error*), dan PSNR (*Peak Signal to Noise Ratio*)**.**

## 1.3. Rumusan Masalah

1. Proses *Cipher Hill* yang telah dimodifikasi pada enkripsi dan dekripsi pesan teks.
2. Proses Steganografi dengan menggunakan metode SSB-4.
3. Proses algoritma *Cipher Hill* yang dimodifikasi dan metode SSB-4 menjadi sistem kombinasi kriptografi dan steganografi.
4. Performansi sistem kombinasi kriptografi dan steganografi yang dibentuk.

## 1.4. Batasan Masalah

1. Metode steganografi yang digunakan yaitu metode SSB-4 sedangkan untuk enkripsi dekripsi menggunakan algoritma *Cipher Hill* yang telah di modifikasi.
2. *Secret messages* merupakan pesan teks yang di enkripsi dekripsi dengan algoritma *Cipher Hill* yang telah dimodifikasi.
3. *Cover-images* berupa citra digital *.bmp (RGB).
4. Implementasi dilakukan dengan menggunakan MATLAB 7.4.0.287 (R2007a).

## 1.5. Metodologi Penulisan

Penulisan Tugas Akhir ini dilakukan dengan melakukan studi literatur, penelitian mandiri, pengumpulan bahan melalui buku-buku referensi, maupun bahan-bahan berbentuk *e-book* dari hasil *googling via internet* serta konsultasi dengan Dosen Pembimbing I dan Pembimbing II.

## 1.6. Sistematika Penulisan

**BAB I PENDAHULUAN**

Menjelaskan latar belakang masalah, tujuan penulisan, rumusan masalah, batasan masalah, metodologi penelitian dan sistematika penulisan.

**BAB II KRIPTOGRAFI DAN STEGANOGRAFI**

Menjelaskan teori pendukung yang menjadi dasar pembahasan. Diantaranya adalah dasar teori Kriptografi, Steganografi, Citra, algoritma *Cipher Hill* dan metode SSB-4.

**BAB III PERANCANGAN DAN IMPLEMENTASI**

Menjelaskan dan menguraikan perancangan sistem kombinasi kriptografi dan steganografi berbasis SSB-4 dengan enkripsi dekripsi pada *text secret messages* menggunakan algoritma *Cipher Hill* yang telah dimodifikasi.

**BAB IV UJI SISTEM DAN ANALISA**

Menguraikan dan menjelaskan proses uji sistem dan analisis hasil pengujian.

**BAB V KESIMPULAN DAN SARAN**

Menguraikan kesimpulan dari hasil analisa dan menjabarkan beberapa saran untuk pengembangan selanjutnya.