**BAB I**

**PENDAHULUAN**

* 1. **Latar Belakang**

Seni adalah indah , merahasiakan sesuatu menjadi lebih indah adalah kunci membangkitkan kemanan dengan sedekat kata sempurna. Indah belum tentu indah, pasalnya algoritma modern yang dikenal ini, telah melewati batas paten selama 20 tahun dan cepat-nya pertumbuhan kecanggihan teknologi menjadi tantangan solusi modern ini adalah melukis RSA. Sulitnya memfaktorkan bilangan besar dan bilangan yang telah di bangkitkan, membuat-nya terkenal. Asymetris adalah sebuta-nya, karena memiliki 2 kunci berbeda yang melakukan encryption dan decryption suatu text menjadi kode rahasia yang bermakna kesenangan tersendiri untuk sebuah computer. Panjang kunci sangat mempesona yaitu mampu hingga 2048 bit. Awal kemunculan algoritma ini hanya menyimpan 678 bit.

Beberapa metode steganografi yang banyak digunakan adalah metode *Least Significant Bit* (LSB), *End Of File* (EOF), *Discrete Wavelet Transform* (DWT), dan *Discrete Cosine Transform* (DCT). LSB merupakan metode paling sederhana dan pesan yang disembunyikan cukup aman. Selain itu, LSB merupakan salah satu metode steganografi yang cepat dan mempunyai kapasitas penyisipan yang cukup besar.

Salah satu media yang sering digunakan dalam steganografi adalah *file* citra digital. Citra digital terbagi dalam dua format berdasarkan jenis kompresinya yaitu *lossless* dan *lossy*. Citra dengan *lossy* memiliki ukuran yang lebih kecil dibandingkan dengan *lossless*. Citra *Lossy* merupakan salah satu format citra digital yang banyak digunakan saat ini.

Di internet gambar yang paling banyak ditemukan adalah citra berformat *lossy*, contohnya adalah JPEG. Namun pada studi tentang steganografi, citra yang paling sering digunakan adalah citra berformat *lossless*. Seperti penelitian yang telah dilakukan oleh Michael Sitorus, Rizky Maynarda, dkk., dan Irpan Adiputra Pardosi, dkk.

Berdasarkan hal tersebut, maka pada penilitian ini akan dilakukan “Implementasi Steganografi Pada Citra Berformat *Lossy* Dengan Metode *Least Significant Bit* (LSB)”.

* 1. **Rumusan Masalah**

Dalam pelaksanaan tugas penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah “Melakukan pembangkitan kunci private pada enkripsi rsa sesuai informasi device”.

* 1. **Tujuan Penelitian**

Dari rumusan masalah tersebut yang menjadi tujuan dari penelitian ini adalah :

1. Menghasilkan kunci *private* yang tidak tetap.
2. Mempertahankan *Plaintext* dari kunci yang ber-ubah.
3. Proses perubahan kunci *private* berhubungan dengan informasi *device* waktu sekarang.
4. Mempertahankan *CipherText* dan *plaintext* menjadi tetap, terhadap kunci yang berbeda
   1. **Batasan Masalah**

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Informasi *device* menggunakan *format* konversi waktu **GMT +7** ( *default* ) dan **GMT + 8**.
2. Membangkitkan bilangan prima dari angka 2 sampai jumlah decimal ascii, pada setiap character “politeknik negeri samarinda” yaitu 2973 , yang menghasilkan sebanyak 397 bilangan prima.
3. Informasi yang akan di enkripsi adalah teks berupa huruf, simbol (“ ?, , , ! , dan $ “).
4. Panjang kunci hanya 2 bit sampai 4 bit
   1. **Manfaat Penelitian**

Penelitian yang dilakukan diharapkan dapat memberikan manfaat bagi pembaca dan penulis antara lain :

1. Dapat memahami tentang algoritma *Riverst Shamir Adleman* dalam membangkitkan kunci private key.
2. Menambah pengetahuan, wawasan, dan pemahaman tentang algoritma *Riverst Shamir Adleman* dalam merahasiakan serta mengaplikasikan ilmu-ilmu yang didapat untuk dikembangkan lebih lanjut.
3. Diharapkan dapat memberi kemudahan dan bermanfaat untuk informasi secara akademis kepada pembaca tentang metode *Riverst Shamir Adleman*.