BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan pesatnya perkembangan teknologi, hadirnya internet dalam kehidupan sehari-hari mengubah beberapa kebiasaan perilaku manusia. Manusia lebih sering berkomunikasi melalui media sosial (dalam jaringan). Hal ini mempunyai dampak positif juga dampak negatif. Salah satu dari dampak negatifnya yaitu maraknya kejahatan dunia maya (*cyber crime*) dengan cara meretas informasi yang bersifat pribadi atau rahasia yang kemudian dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Atas dasar hal tersebut, diperlukan peningkatan keamanan data.

Banyak cara untuk meningkatkan keamanan data. Diantaranya adalah dengan kriptografi dan steganografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya (Munir, 2006). Algoritma kriptografi yang digunakan penulis yaitu *Rivest Shamir Adleman* (RSA) karena sifatnya yang aman dan sulit untuk memecahkan pemfaktoran bilangan yang besar. Kriptografi RSA ini merupakan kriptografi asimetris yang menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Kunci yang digunakan merupakan bilangan yang besar. Namun pada tahun 2002, Durfee mengemukakan bahwa RSA dapat dikriptanalisis menggunakan metode *Lattice.* Selain itu juga, dikemukakan cara lain untuk mengkriptanalis RSA, yaitu *Hastad's Attack, Coppersmith's Attack,* dan *Wiener's Attack*. Pada tahun 2011, Boucinha mengembangkan salah satu cara mengkriptanalis RSA yang sudah pernah dikemukakan sebelumnya oleh peneliti terdahulu, yaitu *Wiener's Attack* dimana peneliti sebelumnya tidak membuktikan beberapa hal. Oleh karena itu, Boucinha mengemukakan hasil temuannya tersebut. Atas dasar hal tersebut, diperlukan peningkatan dalam kriptografi RSA untuk meminimalisir kemungkinan kriptanalisis.

Steganografi adalah suatu metode menyembunyikan pesan rahasia ke dalam suatu media yang lebih besar dengan suatu cara sehingga orang lain tidak

mengetahui isi maupun keberadaan pesan rahasia tersebut (Munir, 2006). Media yang sering digunakan dalam steganografi sebagai *cover* biasanya media gambar (citra digital). Media yang mengandung pesan tersembunyi disebut *stego.* Citra digital ini merupakan salah satu media yang sering digunakan baik secara langsung maupun dalam media sosial. Hal ini yang mendasari penulis untuk menyembunyikan pesan pada media citra digital. Steganografi memiliki dua proses, yaitu *embedding* dan *extracting*. *Embedding* merupakan proses penyisipan pesan ke dalam *cover image*, sedangkan *extracting* merupakan proses mendapatkan pesan yang tersembunyi di dalam *cover image*. Menurut Batarius dan Maslim (2012), dalam steganografi terdapat beberapa metode, yaitu *Least Significant Bit* (LSB), *Discrete Cosine Transform* (DCT), *Discrete Wavelete Transform* (DWT), dan *Peak Signal To Noise Ratio* (PSNR). Metode yang digunakan penulis yaitu *Least Significant Bit* (LSB), karena memiliki beberapa keunggulan, salah satunya adalah hasil akhir dari steganografi tidak akan jauh berbeda dengan gambar yang belum disembunyikan pesan bahkan tidak terlihat perbedaannya secara kasat mata. Metode ini menyembunyikan pesan dalam bit terendah pada citra digital yang digunakan sebagai wadah penampung pesan. Pada tulisan ini, metode LSB yang akan digunakan adalah penyisipan pesan secara acak (*random*).

Menurut Firdaus (2017) pembangkitan kunci RSA dengan tiga buah bilangan prima memiliki keamanan yang lebih tinggi dibandingkan RSA yang standar. Mardhatillah (2017) dalam penelitian sebelumnya yang membahas mengenai metode LSB secara acak tingkat keamanannya lebih tinggi dibandingkan LSB yang tidak secara acak. Arifin dan Oktoviana (2013) menyimpulkan bahwa wadah untuk menyembunyikan pesan yang berupa gambar 24 bit menghasilkan *stego* yang berupa gambar 24 bit.

Berdasarkan uraian di atas, penulis tertarik untuk mengkaji penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB. Kemudian hasil kombinasi tersebut akan dibuat program komputer menggunakan bahasa pemrograman Python 3.7. Oleh karena itu, penulis mengambil judul "**Implementasi Kriptografi *Rivest Shamir Adleman* (RSA) yang Ditingkatkan dan Steganografi *Least Significant Bit* (LSB)**".

1.2 Batasan Penelitian

Batasan penelitian yang digunakan dalam penelitian ini adalah:

1. Pesan yang disembunyikan adalah pesan teks berupa karakter ASCII dimulai dari karakter ke-32 hingga karakter ke-126, karena karakter-karakter tersebut merupakan karakter yang digunakan dalam penulisan pada umumnya.
2. *Cover medi*a berupa gambar berwarna (RGB) dengan format *.png.
3. Metode steganografi yang digunakan adalah LSB secara acak.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan di atas, maka permasalahan yang dapat dirumuskan adalah :

1. Bagaimana penggabungan algoritma kriptografi RSA yang ditingkatkan dan steganografi dengan metode *Least Significant Bit* (LSB)?
2. Bagaimana implementasi penggabungan algoritma kriptografi RSA yang ditingkatkan dan steganografi dengan metode *Least Significant Bit* (LSB) dalam bentuk program komputer menggunakan bahasa pemrograman Python versi 3.7?

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut:

1. Memperoleh algoritma baru dari penggabungan kriptografi RSA yang ditingkatkan dan steganografi dengan metode *Least Significant Bit* (LSB).
2. Memberikan gambaran dari implementasi penggabungan algoritma kriptografi RSA yang ditingkatkan dan steganografi dengan metode *Least Significant Bit* (LSB) dalam bentuk program komputer menggunakan bahasa pemrograman Python versi 3.7.

1.5 Manfaat Penelitian

Manfaat yang hendak dicapai dari penelitian ini adalah memberi kontribusi dalam bidang matematika terapan melalui pengembangan kriptografi dan steganografi dengan menggabungkan kriptografi RSA yang ditingkatkan dan

steganografi LSB dalam bentuk program aplikasi komputer dengan bahasa pemrograman Python versi 3.7.

1.6 Sistematika Penulisan

Penulisan skripsi ini akan dibagi menjadi beberapa bab, yaitu:

1. BAB I PENDAHULUAN

   Bab ini terdiri atas latar belakang, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

2. BAB II LANDASAN TEORI

   Bab ini membahas teori-teori dasar dan konsep yang berhubungan dengan Kriptografi RSA dan Steganografi dengan metode LSB. Teori-teori dasar dan konsep tersebut terdiri dari algoritma kriptografi RSA, teori bilangan, steganografi LSB, sistem ASCII, dan citra digital.

3. BAB III METODE PENELITIAN

   Bab ini menjelaskan desain penelitian yang direncanakan dari perumusan masalah, mengkaji model dasar, mengembangkan model dasar, mengkontrusi program, validasi hingga kesimpulan.

4. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

   Bab ini memuat hasil penelitian mengenai penggabungan kriptografi RSA yang ditingkatkan dan steganografi menggunakan metode LSB. Pada bab ini, dijelaskan mengenai algoritma kriptografi RSA yang ditingkatkan, konsep penggabungan kritografi RSA yang ditingkatkan dengan steganografi dengan metode LSB, dan implementasinya dalam program komputer.

5. BAB V KESIMPULAN DAN SARAN

   Bab ini memuat kesimpulan yang diambil dari hasil penelitian dan saran-saran dari hasil yang didapat.