BAB V
KESIMPULAN DAN SARAN

Berdasarkan rumusan masalah dan hasil penelitian serta pembahasan terhadap hasil penelitian sebagaimana yang diuraikan pada bab sebelumnya maka diperoleh kesimpulan dan saran dari hasil penelitian tersebut.

5.1 Kesimpulan

Berdasarkan penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB memiliki tiga tahapan. Tahapan pertama merupakan pembangkitan kunci publik dan kunci privat yang dibutuhkan untuk melakukan enkripsi dan dekripsi. Pada tahap pembangkitan kunci, dilakukan beberapa langkah berikut.
    1) Pilih tiga buah bilangan prima $p_1, p_2,$ dan p_3 yang apabila dikonversi ke biner akan berukuran 1024-bit.
    2) Hitung $n = p_1 \cdot p_2 \cdot p_3$ ($p_i \neq p_j, i \neq j$ agar n tidak mudah difaktorkan).
    3) Hitung $\phi(n) = (p_1 - 1)(p_2 - 1)(p_3 - 1)$.
    4) Pilih kunci publik $b = 65537$ (kunci publik yang sering digunakan di industri).
    5) Bangkitkan kunci privat a yang memenuhi $a \cdot b \equiv 1 \ (mod\ \phi(n))$

    Tahapan kedua merupakan enkripsi RSA ketika pengirim pesan mengubah *plaintext* menjadi *ciphertext* kemudian disembunyikan ke dalam gambar sehingga dihasilkan *stego image* dengan cara *embedding* LSB secara acak menggunakan PRNG. Tahapan ketiga merupakan *extracting* LSB ketika penerima pesan mengembalikan *ciphertext* dari *stego image* kemudian dekripsi RSA dari *ciphertext* yang diperoleh dan mengolahnya menjadi *plaintext*. Gabungan kriptografi RSA yang ditingkatkan dan steganografi LSB ini dapat meminimalisir terjadinya kriptanalisis karena kunci yang dibangkitkan merupakan bilangan yang

sangat besar sehingga sulit untuk difaktorkan serta *ciphertext* yang disembunyikan secara acak di dalam gambar.

2. Implementasi dari penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB dilakukan dengan mengonstruksi suatu program aplikasi komputer menggunakan bahasa pemrograman Python versi 3.7. Pada tampilannya program tersebut memuat proses pembangkitan kunci, enkripsi dan *embedding*, serta *extracting* dan dekripsi. Program tersebut dapat digunakan oleh pengirim maupun penerima pesan.

5.2 Saran

Setelah melakukan penelitian mengenai penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB, adapun saran dari penulis untuk penelitian selanjutnya, yaitu:

1. Membandingkan kinerja antara penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB dengan penggabungan kriptografi RSA dan steganografi LSB.
2. Mengembangkan program aplikasi komputer dari penggabungan kriptografi RSA yang ditingkatkan dan steganografi LSB menggunakan bahasa pemrograman lain.