

## BAB V

### KESIMPULAN DAN SARAN

Berdasarkan rumusan masalah, dan pembahasan hasil penelitian sebagaimana yang telah dipaparkan pada bab sebelumnya maka diperoleh kesimpulan dan saran dari hasil penelitian tersebut.

#### 5.1 Kesimpulan

Kesimpulan yang diperoleh dari hasil penelitian yang telah diuraikan sebelumnya antara lain sebagai berikut.

1. Skema penggabungan algoritma kriptografi RSA yang ditingkatkan dan AES dimulai dengan adanya perubahan pada pembangkitan kunci, di mana pada algoritma RSA standar digunakan dua bilangan prima, sedangkan pada algoritma kriptografi RSA yang ditingkatkan digunakan tiga bilangan prima, hal ini dapat membuat proses faktorisasi lebih sulit karena harus memfaktorisasi menjadi tiga bilangan. Setelah pembangkitan kunci, skema kriptografi *hybrid* diterapkan pada penggabungan dua algoritma ini di mana kunci publik RSA yang ditingkatkan akan digunakan untuk enkripsi kunci AES sehingga permasalahan transmisi kunci rahasia dalam algoritma AES dapat terselesaikan.
2. Implementasi penggabungan algoritma kriptografi RSA yang ditingkatkan dan AES pada aplikasi pengirim *email* dilakukan dengan mengkonstruksi suatu program aplikasi komputer dengan bahasa pemrograman *python*. Dalam aplikasi tersebut, pengguna dapat melakukan pembangkitan kunci, enkripsi pesan, dekripsi pesan, dan pengiriman *email*.

#### 5.2 Saran

Setelah melakukan penelitian mengenai implementasi penggabungan algoritma kriptografi RSA yang ditingkatkan dan AES pada aplikasi pengirim *email*, terdapat beberapa saran untuk dikembangkan pada penelitian selanjutnya, yaitu:

1. Penggunaan jenis algoritma AES yang lain contohnya seperti AES-256 dan mengkaji kelebihan dan kekurangannya untuk mendapatkan algoritma terbaik.

2. Mengembangkan penggunaan algoritma ini pada objek lain misalnya gambar, ataupun video.