ABSTRAKSI

Penggunaan jaringan komunikasi data antar berbagai sistem komputer telah berkembang pesat diberbagai bidang, sehingga diperlukan adanya sistem yang lain untuk menjaga kerahasian dan keamanan dalam pertukaran data.

Dalam penanganan keamanan dan kerahasiaan data tersebut digunakan algoritma kriptografi untuk melakukan penyandian data, yaitu untuk mengubah data menjadi bentuk yang tidak dapat dipahami oleh orang yang tidak berhak menerima data tersebut. Oleh sebab itu selain kerahasiaan kuncinya, kehandalan algoritma kriptografi yang digunakan juga mempengaruhi kehandalan penanganan keamanan dan kerahasian data dalam sistem komunikasi data tersebut.

Sistem kriptografi, berdasarkan jumlah pemakaian kunci, dapat dibagi dua, yaitu, pertama, kriptografi konvensional yang menggunakan satu kunci dan kedua, kriptografi kunci publik yang menggunakan dua kunci. kriptografi konvensional adalah pengolahan data dengan menggunakan satu buah kunci dan algoritmanya berdasarkan substitusi dan permutasi. Kriptografi kunci publik adalah pengolahan data dengan menggunakan dua kunci yang terpisah dan algoritmanya berdasarkan fungsi-fungsi matematik.Algoritma kriptografi kunci publik yang paling banyak digunakan saat ini adalah algoritma *Rivest Shamir, Adleman (RSA)*.

Dalam tugas akhir ini akan dilakukan pembahasan dalam penggunaan algoritma kriptografi kunci publik, yaitu studi penggunaan algoritma *RSA* untuk penyandian data.