BAB I  
PENDAHULUAN

## Latar Belakang

Kerahasiaan merupakan salah satu aspek penting dari informasi. Penyalahgunaan data yang tidak pada tempat penyimpanan tentunya bisa menimbulkan kerugian yang besar bagi pihak yang mempunyai data dan dokumen tersebut. Salah satu alternatif yang dapat digunakan untuk menjaga kerahasiaan data dan dokumen adalah dengan menyamarkannya ke bentuk tersandi yang tidak bermakna. Hal ini dapat dilakukan dengan menggunakan kriptografi.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan sistem informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Pada prinsipnya, Kriptografi memiliki 4 komponen utama yaitu : *Plaintext*, *Ciphertext*, *Key*, *Algorithm*.

Algoritma yang biasa digunakan untuk memecahkan masalah dalam hal melindungi kerahasian data dalam bentuk file sendiri bermacam-macam. Contoh-nya *Digital Signature Algorithm* (DSA), *Diffie-Hellman* (DH), *ElGamal*, *Elliptic Curve Cryptography* (ECC), dan *Rivest-Shamir-Adleman* (RSA).

Pada penilitian ini akan diterapkan Algoritma Rivest-Shamir-Adleman (RSA) yang akan membantu proses pembentukan enkripsi file teks untuk melindungi data agar tetap aman dari orang-orang yang tidak berhak menyisipkan atau menghapus pesan, data, atau informasi data. Algoritma Rivest-Shamir-Adleman (RSA) termasuk dalam kelompok algoritma asimetris adalah metode yang menggunakan dua kunci berbeda yaitu kunci publik (*public key*) dan kunci privat (*private key*).

## Rumusan Masalah

Dari pembahasan di atas maka dapat dirumuskan pokok permasalahan yaitu: “Bagaimana mengimplementasikan Algoritma RSA untuk mengamankan data yang ada di dalam file teks”.

## Batasan Masalah

Ruang lingkup penelitian akan dibatasi agar penyelesaian masalah dapat lebih terarah pada tujuan tugas akhir ini. Batasan masalah dalam tugas akhir ini adalah :

1. Algoritma yang digunakan adalah RSA.
2. Menggunakan kunci Asimetris.
3. Data yang dienkripsi adalah data yang berbentuk teks di dalam file teks (\*.txt).
4. Pasangan bilangan prima berurutan yang bisa digunakan pada algoritma RSA adalah 11 dan 13.

Beberapa asumsi yang digunakan adalah :

1. Menggunakan tools pemrograman yang sesuai.
2. Kunci Asimetris dimasukkan melalui keyboard terdiri dari kombinasi huruf dan angka.
3. File teks dibuat menggunakan notepad.

## Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Mengimplempentasikan algoritma RSA untuk mengamankan isi file teks.
2. Membangun kunci asimetris yang akan digunakan pada algoritma RSA.

## Manfaat Penelitian

Setelah melakukan penelitian maka diharapkan penelitian akan memiliki manfaat sebagai berikut :

1. Menambah literatur tentang implementasi algoritma RSA untuk keamanan data.
2. Untuk memenuhi syarat mendapatkan gelar derajat Ahli Madya (Amd).