# BAB 1
# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Di zaman modern seperti sekarang, perkembangan teknologi sangat berpengaruh besar terhadap segala aspek kehidupan. Banyak sekali manfaat dan kemudahan yang didapat dengan adanya teknologi yang terus berkembang, salah satunya di bidang informasi dan komunikasi. Dengan adanya internet, semua orang bisa saling berkomunikasi dan bertukar informasi dengan mudah. Namun, hal tersebut juga memiliki dampak buruk karena rawan terjadi pencurian data. Hal ini tentu akan merugikan banyak pihak, terutama bagi pengusaha, pemerintah, bank, dan pihak lain yang memiliki dokumen rahasia. Oleh karena itu, keamanan informasi merupakan faktor penting yang harus dipenuhi. Berbagai cara telah dilakukan untuk mengamankan informasi rahasia tersebut. Salah satu cara yang ditempuh adalah dengan mengubah informasi tersebut menjadi sandi-sandi yang sulit dibaca dan hanya bisa dibaca oleh pihak tertentu, metode ini disebut kriptografi.

Kriptografi merupakan studi matematis yang terkait dengan aspek-aspek yang berhubungan dengan keamanan informasi seperti menyembunyikan isi data, mencegah data dapat dirubah tanpa terdeteksi, ataupun mencegah data digunakan tanpa otoritas yang cukup. Kriptografi dilakukan untuk menyembunyikan konten dari suatu informasi dengan mengubah informasi tersebut menjadi sandi dengan menggunakan kunci, dan untuk membacanya diperlukan kunci pula. Orang yang melakukan proses kriptografi disebut kriptografer. Kebalikan dari kriptografi adalah *Kriptoanalisis,* yaitu seni dan ilmu untuk memecahkan *Chiperteks* menjadi *Plainteks* tanpa melalui cara yang seharusnya, dan orangnya disebut *Kriptoanalis.*

Berdasarkan kerahasiaan kuncinya, algoritma dari kriptografi dapat dibedakan menjadi algoitma sandi kunci rahasia (private key) dan algoritma sandi kunci publik (public key). Namun algoritma kunci publik (public key) lebih sering

digunakan karena penggunaanya yang lebih efisien dari kunci rahasia (private key). Salah satu algoritma kunci publik (public key) yang sering digunakan adalah algoritma Rivest-Shamir-Adleman (RSA). Algoritma RSA dikembangkan oleh Ron (R)ivest, Adi (S)hamir, dan Len (A)dleman dari Massachussets Institute of Technology (MIT) pada tahun 1978. Secara garis besar, algoritma RSA melibatkan perkalian dua bilangan prima yang besar dan dengan tambahan operasi matematika lain menghasilkan dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key). Pembuatan kunci tersebut dilakukan dengan memilih bilangan prima acak yang besar.

Berdasarkan uraian di atas, penulis tertarik untuk mengkaji lebih lanjut algoritma kriptografi Rivest-Shamir-Adleman (RSA). Oleh karena itu, penulis mengambil judul **"Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest-Shamir-Adleman (RSA)".**

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka dibuat beberapa rumusan masalah sebagai berikut.

1. Apa konsep matematis yang melandasi pembentukan algoritma kriptografi RSA?
2. Bagaimana cara kerja algoritma kriptografi RSA dan aplikasinya dalam tanda tangan digital?
3. Bagaimana implementasi algoritma RSA dalam bentuk program yang sederhana?
4. Bagaimana hasil analisis dan perbandingan program implementasi algoritma RSA?

## 1.3 Batasan Masalah

Sesuai dengan judul skripsi ini, pembahasan lebih difokuskan pada algoritma kriptografi RSA yang merupakan bagian dari algorima kriptografi kunci publik. Adapun yang menjadi batasan masalah adalah sebagai berikut :

1. Pembahasan mengenai algoritma kriptografi RSA ini meliputi konsep matematis yang melandasinya.
2. Membahas proses penyandian meliputi pembentukan kunci, enkripsi pesan, dan dekripsi pesan.
3. Pembahasan implementasi RSA pada tanda tangan digital hanya meliputi konsep teoritis.
4. Program yang dibuat merupakan implementasi dari algoritma RSA dengan menggunakan Visual Basic 6.0.

## 1.4 Tujuan Penulisan

Berdasarkan rumusan masalah yang telah diuraikan, maka skripsi ini bertujuan untuk memberikan gambaran mengenai:

1. Konsep matematis yang melandasi pembentukan algoritma kriptografi RSA beserta penerapannya pada tanda tangan digital.
2. Cara kerja algoritma kriptografi RSA dan aplikasinya dalam tanda tangan digital.
3. Implementasi algoritma kriptografi RSA dalam bentuk program yang sederhana.
4. Hasil analisis dan perbandingan program implementasi algoritma RSA

## 1.5 Manfaat Penulisan

Penulis berharap skripsi ini dapat memberi pengetahuan tentang konsep matematis yang melandasi algoritma kriptografi RSA, penerapan pada tanda tangan digital, proses enkripsi dan dekripsi algoritma kriptografi RSA.