# BAB I PENDAHULUAN

## Latar Belakang

Keamanan informasi merupakan hal yang penting, terutama ketika menyangkut privasi seseorang yang tidak boleh diketahui oleh pihak yang tidak di izinkan. Salah satu cara dalam pengamanan data adalah kriptografi atau ilmu penyandian teks.

Selain merupakan ilmu untuk mengamankan data, kriptografi merupakan seni untuk menjaga kerahasiaan data dengan mengubahnya menjadi bentuk tersandi tidak bermakna dan hanya dapat dipecahkan oleh orang yang memiliki kunci.

RSA ( Rivest Shamir Adleman ) merupakan salah satu teknik dalam modern kriptografi yang telah melewati batas paten selama 20 tahun, membuat-nya menjadi mudah di teliti dengan bebas. Sulitnya memfaktorkan bilangan besar menjadi faktor – faktor prima , serta perbedaan kunci dalam penyandian dan penerjemahan membuat RSA menjadi salah satu teknik kriptografi yang sulit dipecahkan. Dengan pesatnya perkembangan teknologi , perlu dilakukan sebuah trik untuk tetap menjadikan RSA sebagai modern kriptografi.

Berdasarkan hal tersebut, maka pada penilitian ini akan dilakukan “Pembangkitan Kunci Private Pada Enkripsi RSA Menggunakan Informasi Device”.

## Rumusan Masalah

Dalam pelaksanaan tugas penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah “Bagaimana Melakukan Pembangkitan Kunci Private Pada Enkripsi RSA Sesuai Informasi Device”.

## Tujuan Penelitian

Dari rumusan masalah tersebut yang menjadi tujuan dari penelitian ini adalah :

1. Menghasilkan kunci *private* yang tidak tetap.
2. Mempertahankan *cipherText* dan *plaintext* terhadap kunci yang berbeda // tidak bisa karena , ada kunci yang jika di faktorkan tidak dapat menerjemahkan beberapa cipher dan tentu kunci lama mampu / bisa men-decrypt.
3. Menjadikan CipherText yang semula tidak rahasia menjadi Rahasia.
4. Menjadikan PlainText yang semula rahasia menjadi Tidak Rahasia.
5. Kunci private tidak bisa di pakai dalam waktu tertentu.

## Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Informasi *device* menggunakan waktu sekarang dan konversi waktu adalah **GMT +7** dan **GMT + 8**.
2. Plaintext dan ciphertext menggunakan ASCII dengan encoding (UTF-8)
3. Panjang kunci adalah 7 bit sampai 14 bit

## Manfaat Penelitian

Penelitian yang dilakukan diharapkan dapat memberikan manfaat bagi pembaca dan penulis antara lain :

1. Menambah pengetahuan, wawasan, dan pemahaman tentang algoritma *Riverst Shamir Adleman* dan mengaplikasikan ilmu-ilmu yang didapat untuk dikembangkan lebih lanjut.
2. Diharapkan dapat memberi kemudahan dan bermanfaat untuk informasi secara akademis.