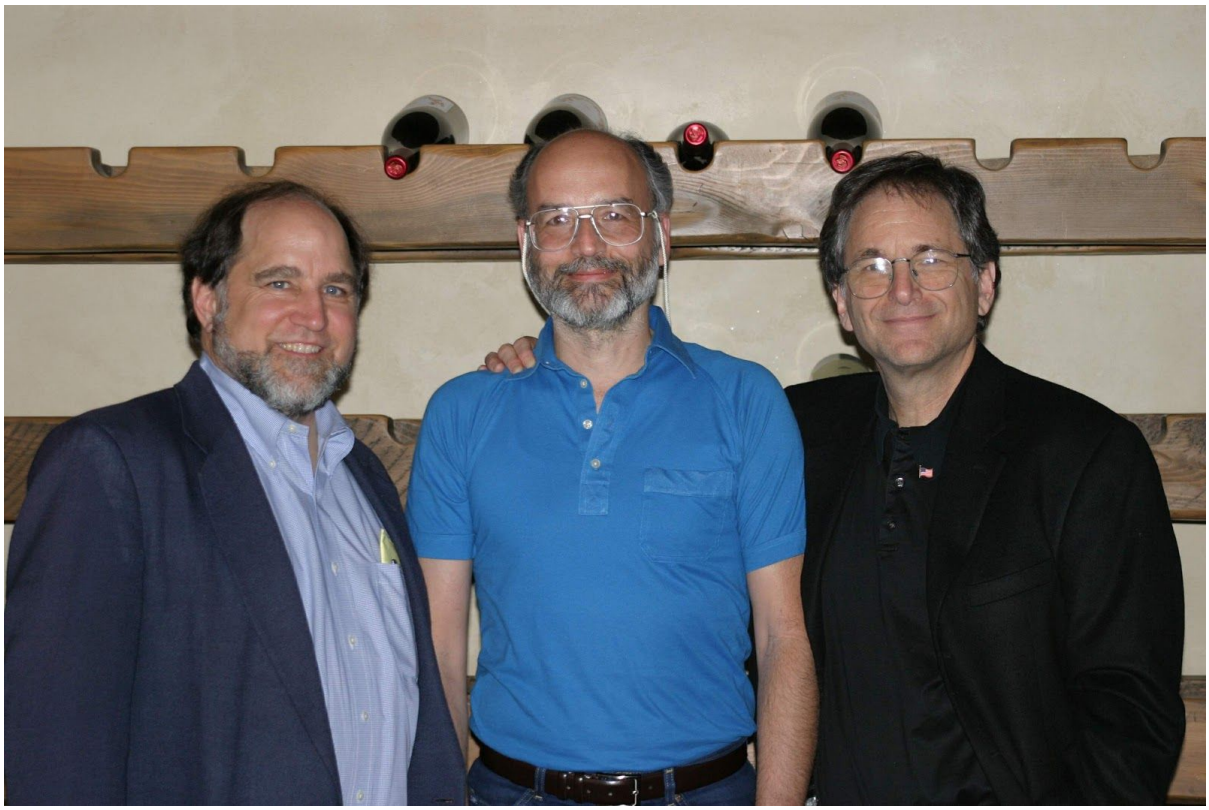
TCC341 - Trabalho 02

Introdução

O RSA é um criptosistema de chave pública criado por Criado publicamente por Ron Rivest, Adi Shamir, and Leonard Adleman em 1977. Sua segurança baseia-se principalmente no problema da fatoração de números grandes.

O SetUp baseia-se simplesmente no acordo do número de bits de n. A geração de chaves começa escolhendo dois primos grandes *p* e *q* e determinando n = p*q. Depois, escolhem-se dois valores e e d, tal que eles sejam inversos multiplicativos no módulo (p-1)(q-1).

Uma mensagem cifrada tem a forma $c = m^e \bmod n$. Já a decriptação deve fazer $m' = c^d \bmod n$.



Objetivo

Nesse trabalho, seu objetivo é quebrar o RSA para valores pequenos de n (4 bytes). Serão dados como entrada 3 números inteiros: o valor de n, o valor de e e um texto cifrado c. Você deve, da maneira que achar melhor, descobrir o valor de m.

Entrada e Saída

Seu programa deve receber 3 inteiros, (n, e, c) representando a chave pública e o texto cifrado e retornar um inteiro m representando a mensagem original.

Exemplos

Nos exemplos abaixo a cor azul representa a entrada que deve ser lida pelo seu programa e a cor vermelha, a saída que deve ser gerada pelo seu programa na saída padrão.

Exemplo 1:

```
143 7 48
9
```

Exemplo 2:

```
2430101 948047 1473513
1070777
```

Exemplo 3:

```
11413 3533 8410
42
```