

# RSA

Por Vinícius "Cabessa" Fernandes dos Santos  Brazil**Timelimit: 1**

O algoritmo RSA é um dos algoritmos de criptografia mais utilizados e é considerado uma das alternativas mais seguras existentes. Seu funcionamento básico é descrito a seguir.

Dois números primos ímpares  $P$  e  $Q$  são escolhidos e calcula-se  $N = PQ$ . A seguir é calculada a função totiente  $\varphi(N) = (P - 1)(Q - 1)$  e um inteiro  $e$  satisfazendo  $1 < e < \varphi(N)$  é escolhido de forma que  $\text{mdc}(\varphi(N), e) = 1$ . Finalmente é calculado o inteiro  $D$ , o inverso multiplicativo de  $e$  módulo  $\varphi(N)$ , ou seja, o inteiro  $D$  satisfazendo  $DE = 1 \pmod{\varphi(N)}$ .

Assim obtemos a chave pública, formada pelo par de inteiros  $N$  e  $E$ , e a chave secreta, formada pelos inteiros  $N$  e  $D$ .

Para criptografar uma mensagem  $M$ , com  $0 < M < N$ , calcula-se  $C = M^e \pmod{N}$ , e  $C$  é a mensagem criptografada. Para descriptografá-la, ou seja, para recuperar a mensagem original, basta calcular  $M = C^d \pmod{N}$ . Note que, para isso, a chave secreta deve ser conhecida, não sendo suficiente o conhecimento da chave pública. Note ainda que a expressão  $x = 1 \pmod{y}$  usada acima equivale a dizer que  $y$  é o menor natural tal que o resto da divisão de  $x$  por  $y$  é 1.

Neste problema você deve escrever um programa para quebrar a criptografia RSA.

## Entrada

A única linha da entrada contém três inteiros  $N$ ,  $E$ , e  $C$ , onde  $15 \leq N \leq 10^9$ ,  $1 \leq E < N$  e  $1 \leq C < N$ , de forma que  $N$  e  $E$  constituem a chave pública do algoritmo RSA descrita acima e  $C$  é uma mensagem criptografada com essa chave pública.

## Saída

Seu programa deve produzir uma única linha, contendo um único inteiro  $M$ ,  $1 \leq M < N$ , a mensagem original.

Exemplo de Entrada	Exemplo de Saída
1073 71 436	726