Homework 05 - Introdução à Criptografia
Problema I da Maratona de Programação da SBC 2015

RSA

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 $\Phi(n) = (p - 1)(q - 1)$ e um inteiro e satisfazendo $1 < e < \Phi(n)$ é escolhido de forma que $mdc(\Phi(n); e) = 1$. Finalmente é calculado o inteiro d, o inverso multiplicativo de e módulo $\Phi(n)$, ou seja, o inteiro d satisfazendo $de = 1 \pmod{\Phi(n)}$.

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.

Exemplos

Entrada	Saída
1073 71 436	726

Entrada	Saída
91 43 19	33