ถอดรหัส

1 second, 32 MB

"ในปัจจุบัน เทคโนโลยีได้ก้าวหน้ากว่าเมื่อก่อนไปมาก เกิดการเข้ารหัสแบบใหม่ที่ เรียกว่า Asymmetrical cryptography หรือ Public-key cryptography ซึ่ง เป็นรูปแบบการเข้ารหัสอันเป็นที่นิยมมาก หนึ่งในระบบการเข้ารหัสแบบนี้คือ RSA Cryptosystem (RSA: Rivest-Shamir-Adleman) (First published in 1977) โดยหลักการของการเข้ารหัสแบบนี้คือ สร้าง private key และ public key แยกกันแล้วส่ง public key ให้เป็นสาธารณะ (ใครจะเข้ามาดู public key ก็ได้ แต่ไม่สามารถดู private key ได้) เมื่อมีคนต้องการส่งข้อความมาหาเราแต่ ไม่อยากให้คนอื่น ๆ รู้ ก็จะต้อง encrypt ข้อความตนเองด้วย public key ก่อน แล้วค่อยส่งมาหาเรา แล้วเราจะต้อง decrypt โดยใช้ private key "

ต่อไปจะเป็นวิธีการสร้าง key ของ RSA cryptosystem

1. เลือกจำนวนเฉพาะ p และ q ที่ไม่เท่ากัน
2. หา $n = pq$
3. หา $j = (p-1)(q-1)$
4. เลือกจำนวนเต็ม e ซึ่ง $1 < e < j$ และ $\gcd(e, j) = 1$
5. หา d ที่ $de \equiv 1 (\mathrm{mod}\ j)$ กล่าวคือ d เป็น modular multiplicative inverse ของ e บนมอดูโล j

หลังจากนั้น e จะเป็น public key exponent ส่วน d จะเป็น private key exponent ต่อมาจะเป็นการ เข้ารหัส - ถอดรหัส (บุคคลภายนอกจำเป้นต้องรู้ e และ n จึงจะเข้ารหัสได้)

- **การเข้ารหัส**
  การเข้ารหัสสามารถกระทำได้โดยการแปลงตัวเลข m ที่จะเข้ารหัส ให้กลายเป็น c โดยที่ $c \equiv m^e (\mathrm{mod}\ n)$
  c จะเป็นรหัสที่ปลอดภัยแล้ว
- **การถอดรหัส**
  การถอดรหัสสามารถกระทำได้โดยการนำตัวเลข c ที่เข้ารหัสไปแล้วมายกกำลัง d ทำให้ได้ c^d แต่
  $c^d \equiv m^{de} \equiv m\ (\mathrm{mod}\ n)$ จึงสามารถหาค่า m ได้ตามต้องการ

วันหนึ่ง น้องปลื้มต้องการส่งจดหมายรักไปให้กับพี่ปิง โดยที่ไม่อยากให้พี่ตาต้ารู้ จึงใช้ระบบ RSA โดยพี่ปิงได้ปล่อยค่า p, q และ e มา และน้องปลื้มมีค่า m อยู่ในใจอยู่แล้ว หลังจากน้องปลื้มได้เข้ารหัสค่า m แล้ว จึงกลายเป็นค่า c ตอนนี้น้องปลื้มกำลังฝึกเขียนโปรแกรม encryption อยู่ แต่พี่ปิงนั้น เอาแต่นอนไปทั้งวันทั้งคืน จึงไม่ได้เขียนโปรแกรมเลย เขาจึงขอให้คุณช่วยเขียนโปรแกรมถอดรหัส RSA จากข้อมูลที่ให้ไป

งานของคุณ

เขียนโปรแกรมถอดรหัส เมื่อคุณทราบ p, q, e, c แล้ว

Input

บรรทัดแรกระบุ T จำนวนเทสเคส

อีก T บรรทัดระบุ p, q, e, c

Output

มี T บรรทัด แต่ละบรรทัด ระบุ จำนวนเต็ม 1 จำนวน แสดงถึงข้อความดั้งเดิมก่อนเข้ารหัส RSA

Constraints

- $1 \leq \mathrm{T} \leq 10^5$
- $1 \leq p, q, e, c \leq 10^9 + 7$
- $1 \leq m < n \leq 10^9$

Sample

Input	Output
1 101 211 11189 5135	12345