

F. 密码学第三次小作业 / Rsa

时间限制： 1.0 秒

空间限制： 512 MB

【题目背景】

1977 年，罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）提出了 RSA 加密算法。RSA 加密算法是一种非对称加密算法，其可靠性由极大整数因数分解的难度决定。换言之，对一极大整数做因数分解愈困难，RSA 算法愈可靠。假如有人找到一种快速因数分解的算法的话，那么用 RSA 加密的信息的可靠性就肯定会极度下降。

RSA 的基本原理如下：

- 公钥与私钥的产生

1. 随机选择两个不同大质数 p 和 q ，计算 $N = p \times q$
2. 根据欧拉函数性质，求得 $r = \varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$
3. 选择一个小于 r 的正整数 e ，使 e 和 r 互质。并求得 e 关于 r 的乘法逆元 d ，有 $ed \equiv 1 \pmod{r}$
4. 将 p 和 q 的记录销毁。此时， (N, e) 是公钥， (N, d) 是私钥。

- 消息加密：首先需要将消息 m 以一个双方约定好的格式转化为一个小于 N ，且与 N 互质的整数 n 。如果消息太长，可以将消息分为几段，这也就是我们所说的块加密，后对于每一部分利用如下公式加密：

$$n^e \equiv c \pmod{N}$$

- 消息解密：利用密钥 d 进行解密

$$c^d \equiv n \pmod{N}$$

【题目描述】

现在有两个用户由于巧合，拥有了相同的模数 N ，但是私钥不同。设两个用户的公钥分别为 e_1 和 e_2 ，且两者互质。明文消息为 m ，密文分别为：

$$c_1 = m^{e_1} \bmod N$$

$$c_2 = m^{e_2} \bmod N$$

现在，一个攻击者截获了 c_1 ， c_2 ， e_1 ， e_2 ， N ，请帮助他恢复出明文 m 。

【输入格式】

从标准输入读入数据。

输入包含多组数据，第一行一个整数 T 表示数据组数，保证 $1 \leq T \leq 10^4$ 。接下来依次描述每组数据，对于每组数据：

- 一行包含五个正整数 c_1, c_2, e_1, e_2, N ，保证 $2^8 < N < 2^{63}$ ， N 有且仅有两个素因子，其余数据严格按照上述 RSA 算法生成。

【输出格式】

输出到标准输出。

对于每组数据，输出 1 行：

- 一个非负整数 m ，请选手务必在输出时保证 $0 \leq m < N$ 。答案 m 保证与 N 互质。

【样例 1 输入】

```
1
1502992813 2511821915 653507 57809 2638352023
```

【样例 1 输出】

```
19260817
```