2019年北邮网安杯线下赛决赛 进行中

添加提问 (/contest/12/clarification/add/)

New Notification: 温馨提示：选手可以多尝试不同的题目 (/contest/12/notification/)

测验首页 (/contest/12/) 提交代码 (/contest/12/submit/) 结果列表 (/contest/12/submission/)

提问列表 (/contest/12/clarification/) 排行榜 (/contest/12/board/)

课程分班 2019年北邮网安杯现场赛

当前时间 2019-03-17 10:28:04 **开始时间** 2019-03-17 08:30:00 **总长** 180 分钟 **剩余** 1:01:55

B. RSA（100分）

运行时间限制: 1000	**运行内存限制:** 65536
作者: admin	**是否specialjudge**: False

题目描述

题目描述

RSA 加密算法是一种非对称加密算法。在公开密钥加密和电子商业中RSA被广泛使用。RSA是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。

Alice想要通过一个不可靠的网络接收Bob的一条私人消息，为了不让其他人窃听Bob向Alice发送的消息，他们想用 RSA 算法来加密消息。

将要发送的信息为 M （为了简化问题，信息M中只包含 $ASCII$ 字符），用 RSA 对信息进行加密，公钥是 (N, e) 。首先要把信息 M 转化成一个整数 T ，使用以下规则进行转换：用二进制的 $ASCII$ 码来表示每个字符，每个字符占 `1 Byte(=8 bit)` ；所有字符组成的整个二进制串代表要加密的信息。例如 M 为 “ `aBc` ”，转化为的二进制串为 `0110 0001 0100 0010`

`0110 0011（\x61\x42\x63）` = `6373987` 。对整数 T 进行加密， 得到加密信息 c ：$c \equiv T^e (Mod\ N)$ 。此外公钥中的 N 有 k $(k > 2, k$ 会在输入时直接给出），则规定每次加密的信息（按照二进制表示）的最大长度为 $(k-2)\ Bytes$ 。长度为 p 的信息 M ，转化为 $p\ Bytes$ 的数字。当 $p > (k-2)$ 时，需要把信息 M 分为 r 组，除最后一组外，其余组的信息长度均为 $(k-2)$ 。每组信息分别用 RSA 算法进行加密，最后共产生 r 个加密后的信息 $c_i, i = 1..r$ ，例如 $k = 7$ ，信息 M 为" `Hello,World!` "，信息 M 被分为三组：" `Hello` "、" `,Worl` "、" `d!` "，分别对三组信息进行加密，得到 $c1, c2, c3$ 。

现在Bob知道Alice的公钥为 (N, e) ，且公钥中 的 N 为 $k\ Bytes (k > 2)$ ，Bob想请你帮他把信息 M 用 RSA 算法加密。

输入格式

第一行有一个整数 N ，公钥中的 N

第二行有一个整数 e ，公钥中的 e

第三行有一个整数 k ，公钥中 N 为 $k\ Bytes$

第四行有一个字符串，信息 M ，信息中可能含有空格

输出格式

第一行输出r，代表信息被分为几组

接下来的 r 行，每行一个整数 c_i ，代表第 i 组加密得到的信息

样例输入1

```
3753080629
1457317325
4
Hello,World!
```

样例输出2

```
6
2820382400
3292780895
843859793
2281440677
3288865383
1002040994
```

数据范围

$e < N < 2^{64}, k < 8, |M| < 3 \times 10^4$

保证信息 M 只含有可打印字符

提交题目 (/contest/12/submit/?index=B)