谜题一

1. 加密算法描述

1）加密对象

加密对象为一段有意义的英文文本，不含空格、标点符号等字符，只包含英文字母。我们将 26 个字母a, b, c, ⋯ , y, z依次对应成整数0,1,2, ⋯ ,25. 假设明文为$p[0]p[1]p[2]\cdots p[l-1]$.

2）密钥

密钥是 m+n 个字母$(a_0, a_1, \cdots, a_{m-1}, k_0, k_1, \cdots, k_{n-1})$，其中$a_i$和26 互素，$\mathrm{i} = 0,1, \cdots, \mathrm{m}-1$.

3）加密过程

循环利用$(a_0, a_1, \cdots, a_{m-1})$和$(k_0, k_1, \cdots, k_{n-1})$进行加密：

$$c[i] = a_{i \bmod m} \cdot p[i] + k_{i \bmod n} \ mod\ 26, \quad i = 0 \text{ to } l\text{-1}.$$

密文为$c[0]c[1]c[2]\cdots c[l-1]$.

4）解密过程

$$p[i] = a^{-1}_{i \bmod m} \cdot (c[i] - k_{i \bmod n}) \ mod\ 26, \quad i = 0 \text{ to } l\text{-1}.$$

2. 攻击方式

唯密文攻击，恢复密钥（字母形式）：你将得到一串密文，要求恢复出对应的明文.

3. 时间限制

20XX 年 10 月 9 日之前完成. 成功满分 16 分，每超一天扣 1 分；

失败保底(5 分)；实在解不出来，可以做理论分析(满分 14 分).

4. 发送方式

答案发送给助教 XX（XXX@XX）.格式：**标**

题：姓名+题号

正文：恢复出的明文

5. 题号

解的谜题题号为：（**系统编号**× 9 + 13） mod 43

以下是系统编号. 例如XX的系统编号是 7 号，题号则是$7 \times 9 + 13 \bmod 43 = 33$

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26