BugkuCTF crypto affine

原创

H4ppyD0g 于 2019-09-15 19:14:45 发布 203 收藏

仿射密码是一种替换密码。它是一个字母对一个字母的。

加密函数是 E(x) = (ax + b) (mod m)，其中a和m互质，m是字母的数目。

解码函数是 D(x) = a^(-1) (x - b) (mod m)，其中 a^(-1)是a在Zm群的乘法逆元。

正面暴力方法

```
>>> flag = "szzyfimhyzd"
>>> flagList = []
>>> for i in flag:
 flagList.append(ord(i)-97)

>>> ansFlag = ""
>>> for i in flagList:
  for j in range(0, 26):
   c = (17 * j - 8) % 26
   if c == i:
    ansFlag += chr(j+97)

>>> ansFlag
'affineshift'
```