BugkuCTF-Crypto题affine

原创

彬彬有礼am_03 于 2021-08-24 21:28:52 发布 52 收藏

分类专栏： # BugkuCTF-Crypto 文章标签： python 安全

本文链接：https://blog.csdn.net/am_03/article/details/119899001

BugkuCTF-Crypto 专栏收录该内容

20 篇文章 1 订阅

订阅专栏

题目描述：

描　　述: y = 17x-8 flag{szzyfimhyzd}

这题考的是仿射密码，了解一下仿射密码

$$e(x) = ax + b \pmod{m}$$

仿射密码为一类替换密码。它是一个字母对一个字母的。它的加密函数为

其a和m互质，m为字母的数目。

解码函数为

$$d(x) = a^{-1}(x - b) \pmod{m}$$

其a^-1为a在Zm群的乘法逆元

乘法逆元：

1	3	5	7	9	11	15	17	19	21	23	25
1	9	21	15	3	19	7	23	11	5	17	25

所有与26互素元素的乘法逆元：

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

解密：y=ax-8，根据乘法逆元推断a=23，通过Python脚本，具体代码如下：

```python
#-*-coding:utf-8-*-
#i=1
#while(17*i%26!=1):
#    i+=1
#求出17的乘法逆元

x='szzyfimhyzd'
#方法一：
for i in range(len(x)):
    print(i,chr(23*(ord(x[i])-ord('a')+8)%26+ord('a')))


#方法二：
for i in range(len(x)):
 temp=23*(ord(x[i])-ord('a')+8)
 temp=temp%26
 result = temp + ord('a')
 print(chr(result),end='')
```

方法三：
逆算法太过复杂，直接去暴力碰撞即可

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'
```