仿射密码 ctf

原创

husb-052 于 2021-10-27 14:31:43 发布 121 收藏

分类专栏： 古典密码 文章标签： 密码学 python

本文链接：https://blog.csdn.net/weixin_49298265/article/details/120992280

仿射密码

> Buuctf- Crypto-[GKCTF2020]小学生的密码学
> e(x)=11x+6(mod26)
> 密文：welcylk

1. 原理

改密码运用乘法逆元和模运算。$a_{Z对应于0}25$， 将明文的每个字符转为对应的数字

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	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

加密函数 E(x)=(a*x+b)(mod 26) a,b为密钥，a必须与26互质
解密函数 D(x)=a^(-1) (x-b)(mod 26) a^(-1) 为a关于26的乘法逆元

2. 分析

已知加密函数e(x)=11x+6(mod 26)。
求出11关于26的乘法逆元19，则D(x)=19*(x-6)(mod 26)

3. 脚本

```
import base64
# 求逆元
from gmpy2 import invert
x= invert(11,26) #x=19为逆元

c = 'welcylk'
m=''
for i in c:
    s = ord(i)-97
    q = chr((((s-6)*x) % 26)+97)
    m+=q

print(m)
print(base64.b64encode(m.encode('utf-8')))
```

4. 答案

flag{ c29yY2VyeQ==}