GKCTF2020笔记

原创

KogRow 于 2021-06-03 15:04:49 发布 55 收藏
分类专栏： Crypto CTF 文章标签： CTF Crypto

Crypto

CTF还是要多做，不然就会吃没见识的亏

1.小学生的密码学

e(x)=11x+6(mod26)

密文：welcylk（flag为base64形式）

这题是典型的仿射密码。**仿射密码**是一种替换密码。它是一个字母对一个字母的。它的加密函数是：

$e(x) = ax + b(mod m)$，其中a和m互质，m是字母的数目。

解密函数是$d(x) = a^{-1}(x - b) \pmod{m}$

其中a^{-1}是a在$\mathbb{Z}m$群的乘法逆元。

上代码：

```
# -*- coding:utf-8 -*-

import string

letters = string.ascii_letters

def encode(plaintext, a, b, m):
    encode_str = ''
    for s in plaintext:
        if s in letters:
            n = letters.find(s) % m
            y = (a * n + b) % m
            if s.isupper():
                y = y + m
            encode_str += letters[y]
        else:
            encode_str += s
    return encode_str

def ext_euclid(a, m):
    if m == 0:
        return 1, 0
    else:
        x, y = ext_euclid(m, a % m)
        x, y = y, (x - (a // m) * y)
        return x,y

def decode(encodes, a, b, m):
    decode_str = ''
    x = ext_euclid(a,m)
    a = x[0]
    if a < 0:
        a = a + m
    for s in encodes:
        if s in letters:
            n = letters.find(s) % m
            y = a * (n - b) % m
            if s.isupper():
                y += m
            decode_str += letters[y]
        else:
            decode_str += s
    return decode_str

if __name__ == '__main__':
    plaintext = 'AFFINE CIPHER'
    a = 11
    b = 6
    m = 26
    s = 'welcylk'
    d = decode(s, a, b, m)
    print ("解密: " + d)
```

解码得到明文sorcery.

然后得到flag{c29yY2VyeQ==}