XCTF crypto新手练习区_1-12

转载

H4ppyD0g 于 2019-07-17 17:03:41 发布 1599 收藏 2

1 base64

把给的字符串用base64在线解码工具解码一下就得出flag。

知识点

Base64编码是从二进制到字符的过程，可用于在HTTP环境下传递较长的标识信息。采用Base64编码具有不可读性，需要解码后才能阅读。

Base64编码规则：
它将每3个字节(3个 字符)（24位）转换为4个字符。因为6位二进制数可以表示64个不同的数，因此只要确定了字符集（含64个字符），并为其中的每个字符确定一个唯一的编码，就可以通过映射将二进制字节转换为Base64编码。

通过每次切出3个字节，最后可能有以下几种情况
没有字节剩下---------->不需要其他操作
还剩下1个字节---------->后面补零，直到位数能被6整除
还剩下2个字节---------->后面补零，直到位数能被6整除

Base64解码规则：
还原时，依次将每4个字符还原成3个字节，最后会出现3种情况之一：
没有字符剩下
还剩下2个字符
还剩下3个字符
这3种情况与上面的3种情况一一对应，只要对补零的过程反过来处理，就可以原样还原了。

---

2 Caesar

用凯撒在线解密工具，第一个字符到c的偏移量作为每个字符的偏移量(14)，得到flag。

知识点

凯撒密码是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。
解密的话就在偏移回去。

---

3 Morse

题解：0对应. 1对应-，去莫尔斯电码在线解码得到flag括号中内容，修改一下即可。

摩尔斯电码（又译为摩斯密码，Morse code）是一种时通时断的信号代码，通过不同的排列顺序来表达不同的英文字母、数字和标点符号。它的代码包括五种： 点、划、点和划之间的停顿、每个字符之间短的停顿、每个词之间中等的停顿以及句子之间长的停顿。
短促的点信号“·”，读“滴”（Di）；保持一定时间的长信号“—”，读“嗒”（Da）。间隔时间：滴，1t；嗒，3t；滴嗒间，1t；字符间，3t；字间，7t。

---

4 Railfence

题解：(复制了一段评论区的大佬的讲话)：ccehg yaefnpeoo be{lcirg} epriec_o ra_g 这样断开，然后12345432123…的回形取每组第一个，提示是分5组，以及flag开头的词组和{以及以}结尾，难点在不是均匀分栏，要自己手动分。

栅栏密码
把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话）

---

5 不仅仅是Morse

先用莫尔斯电码解密
MAY_BE_HAVE_ANOTHER_DECODEHHHHAAAAABAABBBAABBAAAAAAAAABAABABAAAAAAABBABAAABBAAABBA
ABAAAABABAABAAABBABAAABAAABAABABBAABBBABAAABABABBAAABBABAAABAABAABAAAABBABBAABBAA
BAABAAABAABAABAABABAABBABAAAABBABAABBA
很明显前面的东西是假的而后面的东西才是我们应该关心的东西，培根解密后发现是flag。

培根密码
培根密码，又名倍康尼密码（英语：Bacon’s cipher）是由法兰西斯·培根发明的一种隐写术。
加密时，明文中的每个字母都会转换成一组五个英文字母。
加密者需使用两种不同字体，分别代表A和B。准备好一篇包含相同AB字数的假信息后，按照密文格式化假信息，即依密文中每个字母是A还是B分别套用两种字体。
解密时，将上述方法倒转。所有字体一转回A，字体二转回B，以后再按上表拼回字母。

---

6 easy_RSA

RSA加密算法是一种非对称加密算法。（具体是个啥现在还没搞懂）
为了产生两个密钥，选取两个大素数，p和q,为了获得最大程度的安全性，两数的长度一样。计算乘积n=p*q;
随机取加密密钥e,使得e 和（p-1）(q-1) 互素，最后采用扩展欧几里得算法计算解密密钥d，
d=e^-1 mod (p-1)(q-1)
(n,e)是公钥，(n,d)是私钥。

---

7 混合编码

两次base64解码后得到字符的ASCII码，转成字符加上格式就是flag。

---

8 转轮机加密

转轮密码机是由一个输入键盘和一组转轮组成，每个转轮上标有有26个字母，字母的的顺序随意。转轮之间由齿轮进行连接，当一个转轮转动的时候，可以将一个字母转化成另外一个字母。
转轮密码机由多个转轮构成，每个转轮旋转的速度都不一样，比如有3个转轮，分别标号为1,2,3，其中1号转轮转动26个字母后，2号转轮就转动一个字母，当2号转轮转动26个字母后，3号转轮就转动1个字母。因此，当转轮密码机转动26X26X26次后，所有转轮恢复到初始状态，即3个转轮密码机的一个周期长度为26X26X26（17576）的多表代换密码。

```
import re

str = """1: < ZWAXJGDLUBVIQHKYPNTCRMOSFE <
        2: < KPBELNACZDTRXMJQOYHGVSFUWI <
        3: < BDMAIZVRNSJUWFHTEQGYXPLOCK <
        4: < RPLNDVHGFCUKTEBSXQYIZMJWAO <
        5: < IHFRLABEUOTSGJVDKCPMNZQWXY <
        6: < AMKGHIWPNYCJBFZDRUSLOQXVET <
        7: < GWTHSPYBXIZULVKMRAFDCEONJQ <
        8: < NOZUTWDCVRJLXKISEFAPMYGHBQ <
        9: < XPLTDSRFHENYVUBMCQWAOIKZGJ <
        10: < UDNAJFBOWTGVRSCZQKELMXYIHP <
        11: < MNBVCXZQWERTPOIUYALSKDJFHG <
        12: < LVNCMXZPQOWEIURYTASBKJDFHG <
        13: < JZQAWSXCDERFVBGTYHNUMKILOP <"""

# 将str转化为列表形式
# re.S:DOTALL，此模式下，"."的匹配不受限制，可匹配任何字符，包括换行符
content = re.findall(r'< (.*?) <', str, re.S)

print(content)

miwen = 'NFQKSEVOQOFNP'

miyao = [2,3,7,5,13,12,9,1,8,10,4,11,6]

vvv = []
for i in range(13):
    index = content[miyao[i]-1].index(miwen[i])#从0开始
    vvv.append(index)
print(vvv)#密文在通过密钥映射到str里不同的序列中的字符的位置

for i in range(0,26):
    flag=""
    for j in range(13):
        flag += content[miyao[j]-1][(vvv[j]+i)%26]
    print(flag)#这是干啥的不懂
```

cyberpeace{FIREINTHEHOLE}

---

9 Normal_RSA

openssl: 开放式安全套接层协议
OpenSSL 使用 PEM 文件格式存储证书和密钥。PEM 实质上是 Base64 编码的二进制内容，
再加上开始和结束行，如证书文件的
-----BEGIN CERTIFICATE-----
和
-----END CERTIFICATE-----
在这些标记外面可以有额外的信息，如编码内容的文字表示。文件是 ASCII 的，可以用任何文本编辑程序打开它们。

这道题实在不会了，放弃。

---

10 easychallenge

在线反编译pyc后得到源代码，根据加密规则解密得到flag。

```
import base64

final = 'UC7KOWVXWVNKNIC2XCXKHKK2W5NLBKNOUOSK3LNNVWW3E==='

def decode3(ans):
    return base64.b32decode(ans)


def decode2(ans):
    s=''
    for i in ans:
     x=i^36
     x=x-36
     s+=chr(x)
    return s


def decode1(ans):
    s=''
    for i in ans:
        x=ord(i)-25
        x=x^36
        s+=chr(x)
    return s


t1=decode3(final)
print(t1)

t2=decode2(t1)
print(t2)

print(decode1(t2))
```

---

11 幂数加密

二进制幂数加密法

二进制数除了0和1的表示方法外，在由二进制转换成十进制的时候，还可以表示成2的N次方的形式。例如：15=2^0 + 2^1 + 2^2 + 2^3

并且我们发现，任意的十进制数都可以用2^n 或 2^n + 2^m+……的形式表示出来。

把其中的次幂拿出来的牌排列作为这个数的密文的过程就是二进制幂数加密。

题解：这道题根本就不是二进制幂数加密，只是把这串数分开后，每组相加得到字母在字母表的顺序

密文分成： 88421 0122 048 02244 04 0142242 0248 0122

求出根据幂数求出明文。

```python
lt = ["88421","0122","048","02244","04","0142242","0248","0122"]
flag = ''

for i in range(len(lt)):    #len(lt)=8
    list = []
    for j in lt[i]:
        list.append(j)

    ans = 0
    for k in list:
        ans += int(k)
    # 字母ascii值与字母顺序相差为96
    print(ans)
    flag += chr(ans+64)

print('flag is ',flag)
```

---

12 easy_ECC

不会，以后再说 O(∩_∩)O