BUUCTF Crypto3

原创

smile*** 于 2020-04-18 18:30:52 发布 772 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_45784859/article/details/105602386

传感器

题目

5555555595555A65556AA696AA6666666955

这是某压力传感器无线数据包解调后但未解码的报文(hex)

已知其ID为0xFED31F，请继续将报文完整解码，提交hex。

提示1：曼联

思路

曼彻斯特编码（Manchester Encoding），也叫做相位编码（ Phase Encode，简写PE），是一个同步时钟编码技术，被物理层使用来编码一个同步位流的时钟和数据。它在以太网媒介系统中的应用属于数据通信中的两种位同步方法里的自同步法（另一种是外同步法），即接收方利用包含有同步信号的特殊编码从信号自身提取同步信号来锁定自己的时钟脉冲频率，达到同步目的。

将5555555595555A65556AA696AA6666666955转化为二进制，根据01->1,10->0.可以得到

0101->11

0110->10

1010->00

1001->01

将得到的二进制按照上述转换后，对比ID并不重合，根据八位倒序传输协议将二进制每八位reverse，然后转换十六进制就可以得到flag。

思路主要参考：https://www.xmsec.cc/manchester-encode/

代码如下：

```
cipher='5555555595555A65556AA696AA6666666955'
def iee(cipher):
    tmp=''
    for i in range(len(cipher)):
        a=bin(eval('0x'+cipher[i]))[2:].zfill(4)
        tmp=tmp+a[1]+a[3]
        print(tmp)
    plain=[hex(int(tmp[i:i+8][::-1],2))[2:] for i in range(0,len(tmp),8)]
    print(''.join(plain).upper())

iee(cipher)
```

RSAROLL

题目

题目.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

RSA roll! roll! roll!
Only number and a-z
(don't use editor
which MS provide)

{920139713,19}

704796792
752211152
274704164
18414022
368270835
483295235
263072905
459788476
483295235
459788476
663551792
475206804
459788476
428313374
475206804
459788476
425392137
704796792
458265677
341524652
483295235
534149509
425392137
428313374
425392137
341524652
458265677
263072905
483295235
828509797
341524652
425392137

其中n=920139713，e=19

将n分解得到p，q

```
***factors found***

P5 = 49891
P5 = 18443
```

然后分别对下面的每一行进行解密，代码如下：

```
import gmpy2
N,p,q,e=920139713,18443,49891,19
d=gmpy2.invert(e,(p-1)*(q-1))
result=[]

with open("data.txt","r") as f:
    for line in f.readlines():
        line=line.strip('\n')#去掉列表中每一个元素的换行符
        result.append(chr(pow(int(line),d,N)))

for i in result:
    print(i,end='')
```

还原大师

题目

我们得到了一串神秘字符串：TASC?O3RJMV?WDJKX?ZM,问号部分是未知大写字母，为了确定这个神秘字符串，我们通过了其他途径获得了这个字串的32位MD5码。但是我们获得它的32位MD5码也是残缺不全，E903???4DAB???08???51?80??8A?,请猜出神秘字符串的原本模样，并且提交这个字串的32位MD5码作为答案。 注意：得到的 flag 请包上 flag{} 提交

思路

直接进行MD5碰撞，代码如下：

```
import string
import hashlib
a='TASC?O3RJMV?WDJKX?ZM'
b='E903???4DAB????08?????51?80??8A?'
dic1=string.digits+string.ascii_lowercase+string.ascii_uppercase
for i1 in dic1:
 for i2 in dic1:
  for i3 in dic1:
   bb='TASC'+i1+'O3RJMV'+i2+'WDJKX'+i3+'ZM'
   aa=hashlib.md5(bb.encode('utf-8'))
   bbb=aa.hexdigest()
   if bbb[:5]=='e9032':
    print(i1+i2+i3)

a=hashlib.md5('TASCJO3RJMVKWDJKXLZM'.encode('utf-8'))
print (a.hexdigest())
```