1.RSA

factordb分解n

然后rsa解密

代码如下：

```
from Crypto.Util.number import *

p=112391349878049935867635590281872450576525502195152017686447707338690881853207409384501788161383948443297233114335498994997957756559212616640879970972948 13

q=120229126614209415925697517318026393750884274634301622521130826196178370109130025154502236569428363780411221638333590979109356384234640062528142669591289 53

phi=(p-1)*(q-1)

e=65537

d=inverse(e,phi)

c=110674792674017748243232351185896019660434718342001686906527789876264976328686134101972125493938434992787002915562500475480693297360867681000092725583284616353543422388489208114545007138606543678040798651836027433383282177081034151589935024292017207209056829250152219183518400364871109559825679273502274955582

n=135127138348299757374196447062640858416920350098320099993115949719051354213545596643216739555453946196078110834726375475981791223069451364024181952818056802089567064926510294124594174478123216516600368334763849206942942824711531334239106807454086389211139153023662266125937481669520771879355089997671125020789

m=pow(c,d,n)

print(long_to_bytes(m))
```

2.Be stream

看到water是256域下的，就把所有数都放在256域之下。构造列表stream，发现stream[i]==stream[i%256]，所以water就能计算了。

代码如下：

```
key = [int.from_bytes(b"Be water", 'big'), int.from_bytes(b"my friend", 'big')]

stream=[]

stream.append(key[0]%256)

stream.append(key[1]%256)

flag=b''

for i in range(2,256):

  stream.append((stream[i-2]*7 + stream[i-1]*4)%256)

flag=b''

enc=b'\x1a\x15\x05\t\x17\t\xf5\xa2-\x06\xec\xed\x01-\xc7\xcc2\x1eXA\x1c\x157[\x06\x13/!-\x0b\xd4\x91-\x06\x8b\xd4-\x1e+*\x15-pm\x1f\x17\x1bY'
```

```
for i in range(len(enc)):
  water = stream[(i//2)**6%256]
  flag += bytes([water ^ enc[i]])
print(flag)
```

3.神秘的电话

莫斯密码，音频转文字后为密文，用base64转换txt文件中的内容，发现是栅栏密码。