week2

crypto

whitegiveRSA

1.题目如下

N = 882564595536224140639625987659416029426239230804614613279163
e = 65537
c = 747831491353896780365654517748216624798517769637260742155527

2.查阅RSA定义

RSA算法的具体描述如下： [5]

（1）任意选取两个不同的大素数p和q计算乘积$n=pq,\varphi(n)=(p-1)(q-1)$ [5]；

（2）任意选取一个大整数e，满足$gcd(e,\varphi(n))=1$，整数e用做加密钥（注意：e的选取是很容易的，例如，所有大于p和q的素数都可用） [5]；

（3）确定的解密钥d，满足$(de)mod\varphi(n)=1$，即$de=k\varphi(n)+1,k\geq 1$是一个任意的整数；所以，若知道e和$\varphi(n)$，则很容易计算出d [5]；

（4）公开整数n和e，秘密保存d [5]；

（5）将明文m（m<n是一个整数）加密成密文c，加密算法为 [5]

$$c=E(m)=m^e modn$$

（6）将密文c解密为明文m，解密算法为 [5]

$$m=D(c)=c^d modn$$

然而只根据n和e（注意：不是p和q）要计算出d是不可能的。因此，任何人都可对明文进行加密，但只有授权用户（知道d）才可对密文解密 [5]。

3.显而易见的解法是因式分解出p，q。通过http://www.factordb.com/得出p，q

4.查阅前人的代码

5.运用python，代码如下

“

```
import libnum
from Crypto.Util.number import long_to_bytes

c = 747831491353896780365654517748216624798517769637260742155527
n = 882564595536224140639625987659416029426239230804614613279163
# n = int("",16)
e = 65537
# e = int("",16)
q = 857504083339712752489993810777
p = 1029224947942998075080348647219

d = libnum.invmod(e, (p - 1) * (q - 1))
m = pow(c, d, n)  # m 的十进制形式
string = long_to_bytes(m)  # m明文
```

```
print(string)  # 结果为 b‘ m ’ 的形式
```

(代码转自https://blog.csdn.net/vhkjhwbs/article/details/101160822)