Assignment # 6

Homework

Homework problems are a preparation for the quizzes. They are *not* graded. Please use the `mywpi` forum to post questions you have on these problems.

- 7.1, 7.2, 7.3, 7.4, 7.5, 7.9, 7.11

Project

Note: For submissions on `mywpi`: Please submit a single pdf file containing your results. Please submit source code as a separate file, but make sure to have it listed in the pdf as well.

1. 7.12

2. Let $N = pq$ be the product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q efficiently.
(*Hint:* Derive a quadratic equation (over the integers) in the unknown p)
Test your method on the following values:

```
N =
20722315404396508870121075604512656462719793460016435638516039926377 1929\
99148340899333780074432633310313712413453406887290801182751289715739 0544\
59639711785124245407361909282954031219576829233479199869259511078148 2773\
59560221916989757577639752257934439408029233229609653485905360877082 3602\
96496661185383062047092207691598917427765692572659335311952888741208 4256\
74377840939137696204915017404504167022305127285450988307879448817234 8520\
36998287050427994833546339406914391130110789245548860819325181924152 6996\
49121115874378686217161806574666956584319584550606271079763874302744 4024\
272132655573187907862317983632445258804 67

phi(N)=
20722315404396508870121075604512656462719793460016435638516039926377 1929\
99148340899333780074432633310313712413453406887290801182751289715739 0544\
59639711785124245407361909282954031219576829233479199869259511078148 2773\
59560221916989757577639752257934439408029233229609653485905360877082 3602\
96496661185383062046800969079228536207671380167394103267336952031670 2623\
30507425932721884259948563226040666972061237157842513975835618072091 1055\
08248305655758745955058204557235328865085763112338933609604396365932 7817\
40006487057672482013153794568033136652355399728037252342909190814086 7101\
582166770468562424701524841906798647864 00
```

If you need to find an integer square root, feel free to use the following code:

```
def intSqrt(square):
    ''' returns the integer square root of square
        if it exists, otherwise the closest
        integer smaller than the square root'''
    import math
    bits = int(math.log(square,2)//2)
    sqrt = 2**bits
    for idx in range(bits,-1,-1):
        if ((sqrt+2**idx)**2 <= square):
            sqrt = sqrt +2**idx
    return sqrt
```

3. Implement padded RSA, as introduced in class. Assume that the message m is always a 256 bit key, i.e. $|m| = 256$ and that $|N| = 1024$ bit.
   (a) What is the length of the random pad r?
   (b) Implement the key generation algorithm that returns a public and a private RSA key, with a modulus size of 1024 bits.
   (c) Implement an padded RSA encryption algorithm that processes messages of 32 byte (256 bit) length.
   (d) Implement the corresponding padded RSA decryption algorithm. Test both functions on random 256 bit keys.

4. In this question you will become familiar with real world usage of public key encryption. The goal is to send a correctly encrypted email to ece4802@WPI.EDU, containing your name and explain why you might need to use this method to send an email to someone. Your email should be encrypted using the public key available in `mywpi`.
   The most popular tool for email encryption builds on GNU PG or gpg2. If you use Thunderbird, then you can install a software for managing the public and private keys such as gpg, together with the Thunderbird extension Enigmail. Windows users might consider gpg4Win. An alternative software for web mail is Mailvelope. If you need more help during these steps or if you are using MAC operating system, please check out the manual from wefightcensorship.org.

Good Luck and Have Fun!