Feedback — Week 6 - Programming Assignment [optional: extra credit]

Help

You submitted this homework on **Sat 10 May 2014 11:57 PM PDT**. You got a score of **4.00** out of **4.00**.

Question 1

Your goal in this project is to break RSA when the public modulus N is generated incorrectly. This should serve as yet another reminder not to implement crypto primitives yourself.

Normally, the primes that comprise an RSA modulus are generated independently of one another. But suppose a developer decides to generate the first prime p by choosing a random number R and scanning for a prime close by. The second prime q is generated by scanning for some other random prime also close to R. We show that the resulting RSA modulus $N = pq$ can be easily factored.

Suppose you are given a composite N and are told that N is a product of two relatively close primes p and q, namely p and q satisfy

$$|p - q| < 2N^{1/4} \quad (*)$$

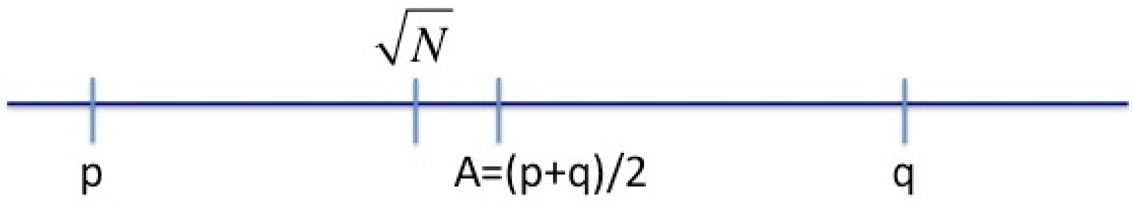
Your goal is to factor N.

Let A be the arithmetic average of the two primes, that is $A = \frac{p+q}{2}$. Since p and q are odd, we know that $p + q$ is even and therefore A is an integer.

To factor N you first observe that under condition (*) the quantity $\sqrt{N}$ is very close to A. In particular

$$A - \sqrt{N} < 1$$

as shown below. But since A is an integer, rounding $\sqrt{N}$ up to the closest integer reveals the value of A. In code, $A = \mathrm{ceil}(\mathrm{sqrt}(N))$where "ceil" is the ceiling function. Visually, the numbers $p, q, \sqrt{N}$ and A are ordered as follows:



Since A is the exact mid-point between p and q there is an integer x such that $p = A - x$and $q = A + x$ But then $N = pq = (A-x)(A+x) = A^2 - x^2$and therefore $x = \sqrt{A^2 - N}$
Now, given x and A you can find the factors p and q of N since $p = A - x$and $q = A + x$

In the following challenges, you will factor the given moduli using the method outlined above. To solve this assignment it is best to use an environment that supports multi-precision arithmetic and square roots. In Python you could use the gmpy2 module. In C you can use GMP.

Factoring challenge #1: The following modulus N is a products of two primes p and q where $|p - q| < 2N^{1/4}$. Find the smaller of the two factors and enter it as a decimal integer.

```
N = 179769313486231590772930519078902473361797697894230657273430081157 \
    73267580550562068698537944921298295958550138753716401571013985864 \
    78337786069255834975410851965916151280575759407526350074759352887 \
    10823649949940771895617054361149474865046711015101563940680527540 \
    071584560878577663743040086340742855278549092581
```

Factoring challenge #2: The following modulus N is a products of two primes p and q where $|p - q| < 2^{11} N^{1/4}$. Find the smaller of the two factors and enter it as a decimal integer.
Hint: in this case $A - \sqrt{N} < 2^{20}$so try scanning for A from $\sqrt{N}$ upwards, until you succeed in factoring N.

```
N = 648455842808071669662824265346772278726343720706976263060439070378 \
    97308618081116462714015276061417569195587321840254520655424906719 \
    89242884484183935328197298853131051173864896596258282150250499026 \
    44521008852816733037111422964210278402893076574586452336833570778 \
    346897158386460882396402368662522117900857 87877
```

Factoring challenge #3: (extra credit) The following modulus N is a products of two primes p and

q where $|3p-2q| < N^{1/4}$. Find the smaller of the two factors and enter it as a decimal integer. Hint: use the calculation below to show that $\sqrt{6N}$ is close to $\frac{3p+2q}{2}$ and then adapt the method above to factor N.

```
N = 720062263747350425279564435525583738338084451473999841826653057981916 \
    355690188337790423408664187663938485175264994017897083524079135686 \
    877441155132015188279331812309091996246361896836573643119174094961348 \
    524639707885238799396839230364676670221627018353299443241192173812 72 \
    9276147530748597302192751375739387929
```

The only remaining mystery is why $A - \sqrt{N} < 1$ This follows from the following simple calculation. First observe that

$$A^2 - N = \left(\frac{p+q}{2}\right)^2 - N = \frac{p^2+2N+q^2}{4} - N = \frac{p^2-2N+q^2}{4} = (p-q)^2/4$$

Now, since for all $x, y:\quad (x-y)(x+y) = x^2 - y^2$ we obtain

$$A - \sqrt{N} = (A - \sqrt{N})\frac{A+\sqrt{N}}{A+\sqrt{N}} = \frac{A^2-N}{A+\sqrt{N}} = \frac{(p-q)^2/4}{A+\sqrt{N}}$$

and since $\sqrt{N} \le A$ it follows that

$$A - \sqrt{N} \le \frac{(p-q)^2/4}{2\sqrt{N}} = \frac{(p-q)^2}{8\sqrt{N}}$$

By assumption (*) we know that $(p-q)^2 < 4\sqrt{N}$ and therefore

$$A - \sqrt{N} \le \frac{4\sqrt{N}}{8\sqrt{N}} = 1/2$$

as required.

Further reading: the method described above is a greatly simplified version of a much more general result on factoring when the high order bits of the prime factor are known.

Enter the answer for factoring challenge #1 in the box below:

You entered:

13407807929942597099574024998205846127479365820592393377723561443721764030073662768891111614362326998675040546094339320838419523375986027530441562135724301

Your Answer		Score	Explanation
13407807929942597099574024998205846127479365820592393377723561443721764030073662768891111614362326998675040546094339320838419523375986027530441562135724301	✓	1.00	

Total	1.00 / 1.00

Question 2

Enter the answer for factoring challenge #2 in the box below:

You entered:

25464796146996183438008816563973942229341454268524157846328581927885777969985222835143851073249573454107384461557193173304497244814071505790566593206419759

Your Answer		Score	Explanation
25464796146996183438008816563973942229341454268524157846328581927885777969985222835143851073249573454107384461557193173304497244814071505790566593206419759	✓	1.00	
Total		1.00 / 1.00	

Question 3

Enter the answer for factoring challenge #3 in the box below:

You entered:

21909849592475533092273988531583955898982176093344929030099423584127212078126150044721102570957812665127475051465088833555993294644190955293613411658629209

Your Answer		Score	Explanation
21909849592475533092273988531583955898982176093344929030099423584127212078126150044721102570957812665127475051465088833555993294644190955293613411658629209	✓	1.00	
Total		1.00 / 1.00	

Question 4

The challenge ciphertext provided below is the result of encrypting a short secret ASCII plaintext using the RSA modulus given in the first factorization challenge. The encryption exponent used is $e = 65537$. The ASCII plaintext was encoded using PKCS v1.5 before the RSA function was applied, as described in Lecture 11.4.

Use the factorization you obtained for this RSA modulus to decrypt this challenge ciphertext and enter the resulting English plaintext in the box below. Recall that the factorization of N enables you to compute $\varphi(N)$ from which you can obtain the RSA decryption exponent.

```
Challenge ciphertext (as a decimal integer):
22096451867410381776306561134883418017410069787892831071731839143676135600120538004282
32965047350942434394621975151225646583996794288946076454204058156474898801373486412045
23252293201764879166664029975091887299716905260832220677716000193292608700095799937
240774589677736978175712672299511486629596279347915 40
```

After you use the decryption exponent to decrypt the challenge ciphertext you will obtain a PKCS1 encoded plaintext. To undo the encoding it is best to write the decrypted value in hex. You will observe that the number starts with a '0x02' followed by many random non-zero digits. Look for the '0x00' separator and the digits following this separator are the ASCII letters of the plaintext. (note: the separator used here is '0x00', not '0xFF' as stated in the lecture)

You entered:

Factoring lets us break RSA.

Your Answer		Score	Explanation
Factoring lets us break RSA.	✓	1.00	
Total		1.00 / 1.00	