MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 08 SOLUTIONS

Deadline: Thursday, 10 November 2016 at 3:05pm
This mission covers Sections 6.1 and 6.2.

1. Graded Problems

1. Work through the RSA code (RSA.sagews) on Moodle.
   a. Notice that if you run the code multiple times, you will end up getting different encrypted text. In a sentence or two, explain why this is:

> Random numbers are generated as part of the algorithm.

   b. Encrypt a one-line phrase, and email the input and output to me (please don't write this one by hand!).
2. Part of the RSA lectures was a claim that we can factor $n = pq$ by just knowing n and $\varphi(n)$ (see notes on using a certain polynomial and the quadratic formula). Write out the details of how you would do this for $n = 27679$. You can use SageMath for the Euler phi function, but you cannot use it for direct factoring here.

$$X^2 - (n - \varphi(n) + 1)X + n \Rightarrow X^2 - 400X + 27679$$
$$X = \frac{400 \pm \sqrt{(-400)^2 - 4(1)(27679)}}{2}$$
$$= 311, 89$$

3. Part of the discussion on RSA attacks was a mention of **continued fractions**.
   a. Read the intro, motivation and notation, and basic formula sections on Wikipedia's continued fractions page: `https://en.wikipedia.org/wiki/Continued_fraction`.

   b. Write an example of a finite continued fraction here.

$$\frac{26}{7} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}$$

   c. Explain in a sentence which types of numbers would have an infinite continued fraction.

> An irrational number would yield an infinite continued fraction.