CRYPTOGRAPHY MISSION 08 DOSSIER

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

Check one:

□ I received help from the following classmate(s) on this assignment:

____.

□ I did not receive any help on this assignment.

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:

   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.

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.

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

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 6.8: # 1, 3
- Section 6.9: # 1, 2