CRYPTOGRAPHY MISSION 08

Deadline: Thursday, 2 November 2017 at 10:50am

This mission covers Sections 6.1, 6.2, 6.3, and 6.4.

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. (Final Project) Write down a short paragraph summary of your project and any team members here. Remember that Dr. Ho assigned you a general topic, but you can choose your own team or work individually within that group.

2. Work through the RSA code here: `https://tinyurl.com/fa17-crypto-rsa`. Notice that if you run the code multiple times, you will end up getting different encrypted text.

   a. In a sentence or two, explain why this is:

   b. Encrypt a one-line phrase, and email the input and output to Dr. Ho (please don't write this one by hand!).

3. Part of the RSA lectures was a claim that we can factor $n = pq$ by just knowing n and $\varphi(n)$. We do this by setting up the quadratic equation $X^2 - (n - \varphi(n) + 1)X + n$ and solving for its roots. Write out the details of how you would do this for $n = 27679$. You can use CoCalc for the Euler phi function, but show the details of the rest of your work.

4. Read through the Miller-Rabin Primality Test (6.3 p. 178). Work through the example. Then, use the primality test for $n = 101$.

5. Use the Fermat Factoring method to factor 70747.

6. Use the $p-1$ Factoring Algorithm to factor 4757. You can use CoCalc to help with the computations.

7. (Honors) Read Sections 6.5 (The RSA Challenge) and 6.6 (An Application to Treaty Verification). Summarize both sections in a short paragraph each.

2. Recommended Exercises

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

- Section 6.8: # 1, 3, 5, 7, 13, 19
- Section 6.9 # 1, 2, 5, 7