MATH/CSCI 408 Name: ______________________________

CRYPTOGRAPHY MISSION 09 DOSSIER

Deadline: Thursday, 17 November 2016 at 3:05pm

This mission covers Sections 6.3, 6.4, and 7.1

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. Read through the Miller-Rabin Primality Test (6.3 p. 178). Work through the example, and write a new example here.

2. Use the Fermat Factoring method to factor 70747.

3. Use the $p-1$ Factoring Algorithm to factor 4757.

4. Use SageMath's `factor()` to check your answers to problems 1 and 2.

5. Given $p = 17$. Solve the following discrete logs problems if possible. If not, explain why.
   a. $14 \equiv 3^x \mod 17$

b. $5 \equiv 4^x \mod 17$

2. Recommended Exercises

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

- Section 6.8: # 9, 13, 18
- Section 6.9: # 11