MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 07 DOSSIER

Deadline: Thursday, 3 November 2016 at 3:05pm
This mission covers Sections 4.2, 4.4, and 4.8.

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. This problem will walk you through a couple of steps of the DES that are different from the Simplified DES model. Read the DES section in the textbook (Section 4.4–skip 4.4.1).
   a. In a couple of sentences and with an example, explain what the Initial Permutation step does.

   b. In a couple of sentences, explain how the keys $K_1, K_2, \cdots, K_{16}$ are generated given a key K.

c. If $B_1 = 101010$, explain how you would use the first S-box S_1 to get an output.

2. Play with the Simplified DES code (found on Moodle as Simple DES.sagews). Specifically, type in a 12-bit input `100100100100`, a key $K =$ `111111110`, and 7 rounds. Write your output here:

3. Read the password security section in the book (Section 4.8).
   a. Explain in a sentence or two what **salt** means in this context. Provide an example:

b. Based on the PDF slides from class (also on Moodle), explain why `GreatPassword123` is a bad password. Be sure to explain what kind of attack might be used to crack this password easily.

2. Recommended Exercises

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

- Section 4.9: # 1, 5
- Section 4.10: # 1