MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 07 DOSSIER

Deadline: Thursday, 19 October 2017 at 10:50am
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. 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 lecture (or the "DES, AES, and Passwords" PDF 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.

3. For a bit string S, let $\bar{S}$ denote the complement of the string by changing all 1s to 0s and 0s to 1s (equivalently, this can be defined as $\bar{S} = S \oplus 1111\cdots$). Show with an explicit example that if the simplified DES key K encrypts a plaintext P to a ciphertext C, then $\bar{K}$ encrypts $\bar{P}$ to $\bar{C}$. You can use the code `https://tinyurl.com/fa17-crypto-DES` again.

4. (Honors) Consider the following DES-like encryption method: Start with a 6-bit message. Divide it into two blocks of length 3 (a left half and a right half): M_0M_1. The key K consists of 3 bits. One round of encryption starts with a pair M_jM_{j+1} and the output is the pair $M_{j+1}M_{j+2}$ where $M_{j+2} = M_j \oplus K$ (where the operation is exclusive or, aka addition mod2). This is done for m rounds, so the ciphertext is M_mM_{m+1}.
   a. Suppose the initial input is 000111 and the key is $K = 101$. What is the ciphertext M_3M_4?

   b. If you have a machine that does the m-round encryption, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} (with the same key K)? Show this explicitly with the example from part (a).

2. Recommended Exercises

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

- Section 4.9: # 2, 7