MATH/CSCI 408 Name: ____________________

CRYPTOGRAPHY MISSION 07 SOLUTIONS

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

This mission covers Sections 4.2, 4.4, and 4.8.

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.

Using the table, the Initial Permutation jumbles the message. For example, the 58th bit becomes the 1st bit, then the 50th bit is the 2nd bit, etc. (following the order of the table.)

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

First the parity bits of K are discarded. Then, the keys $K_1, K_2, \cdots, K_{16}$ are generated by permuting the remaining bits using the table (again, the 57th bit becomes the 1st, the 49th becomes the 2nd, etc.).

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

The first and last bits `10` give the row, and the other four bits give the column in S-Box 1. In this case, we end up with the 3rd row and the 11th column, or 9, which is `1001` in binary.

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:

`011000010101`

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:

Salt means adding in random extra bits to pad a message. For example, if a message if `101010`, then adding in additional bits would give something like `101110100`.

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.

This is a terrible password because it uses common phrases and sequential numbers. A Dictionary Attack or Brute Force Attack would both crack this password very quickly.