MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 03 SOLUTIONS

Deadline: Thursday, 15 September 2016 at 3:05pm
This mission covers Sections 2.8, 2.9, 2.10, and all Classical Ciphers.

1. Graded Problems

1. Read through the "Examples of basic usage" section for Python's pseudo-random number generators (`https://docs.python.org/2/library/random.html`).
   a. In SageMath, generate 5 pseudo-random numbers using `random()`, and write them here (round to 4 decimal places).

> 0.8384, 0.1998, 0.2668, 0.2085, 0.5690

   b. Write down the code for generating a random integer from 1 to 100. Generate 3 such numbers and write them here.

> `randint(1,100)`; 12, 83, 20

   c. Write down the code for generating a random odd from 1 to 101. Generate 3 such numbers and write them here.

> `randrange(1, 101, 2)`; 25, 73, 1

2. Bletchley Park was where a lot of cryptography happened during World War II. Watch `https://www.youtube.com/watch?v=wlWVpOzgrL4`, and write down two facts that you learned here.

> - Alastair Denniston was the first head of the Government Code and Cypher School.
> - Alan Turing knew Enigma could be broken using a brute force strategy.
> - Enigma had a flaw, which is that a letter couldn't be encoded as itself.
> - There were over "150 million million million" possible combinations on an Enigma machine.

3. If `11010010` is your plaintext message, and `10101010` is the key, what is the ciphertext using a One-Time Pad?

> 11010010+10101010 = `01111000`

4. Make a list of all the Classical Ciphers we have covered so far to remember what they are. These might be used in the "Escape Room" activity on 9/15.

> - Shift
> - Affine
> - Vigenère

- Substitution
- Dancing Men
- Playfair
- Block (in particular, Hill)
- Pigpen
- One-Time Pads