CRYPTOGRAPHY MISSION 04 DOSSIER

Deadline: Thursday, 14 September 2017 at 10:50am
This mission covers Sections 2.7 and 2.9.

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. (T & W 2.13 # 14) The ciphertext GEZXDS was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is solved. Find the encryption matrix M.

2. (T & W 2.13 # 16)

   a. The ciphertext ELNI was encrypted by a Hill cipher with a 2×2 matrix. The plaintext is dont. Find the encryption matrix M.

   b. Suppose the ciphertext is ELNK and the plaintext is still dont. Find the encryption matrix. Note that the second column of the matrix is changed. This shows that the entire second column of the encryption matrix is involved in obtaining the last character of the ciphertext.

3. 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).

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

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

4. 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.

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

6. (Honors) Let a, b, c, d, e, f be integers mod26. Consider the following combination of the Hill and affine ciphers: represent a block of plaintext as a pair (x, y) mod 26. The corresponding ciphertext (u, v) is

$$(x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e, f) \equiv (u, v) \bmod 26.$$

Encrypt the plaintext `carolina` using the values below:

$$(x, y)\begin{pmatrix} 3 & 4 \\ 3 & 1 \end{pmatrix} + (8, 11) \equiv (u, v) \bmod 26$$

2. Recommended Exercises

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

- Section 2.13: # 13, 15, 17, 19
- Section 2.14: # 9