CRYPTOGRAPHY MISSION 02 DOSSIER

Deadline: Thursday, 8 September 2016 at 3:05pm
This mission covers Sections 2.4, 2.6, and 2.7.

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. Read the Wikipedia article on the Pigpen cipher:
`https://en.wikipedia.org/wiki/Pigpen_cipher`.
   a. Replicate the set of all graphical symbols on your homework here:

   b. Encrypt the message "you only live twice" using the Pigpen cipher.

2. On Moodle, download and work through the "Encryption.sagews" code.

   a. Using the Caesar cipher with a shift of 12, encrypt "Julius No".

   b. Follow the link mentioned in the SageMath code (recopied here: `http://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/classical.html`). Read through the documentation of the TranspositionCipher. In a sentence or two, describe what the Transposition Cipher does to a plaintext phrase:

   c. Use some SageMath code and the Transposition Cipher to encrypt: "`BABOUTHEOCELOT`" (note that normally, we use lowercase for plaintext, but we need all caps for this particular line of code).

3. (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.

4. (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.

2. Recommended Exercises

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

- Section 2.13: # 13, 17, 24
- Section 2.14: # 10