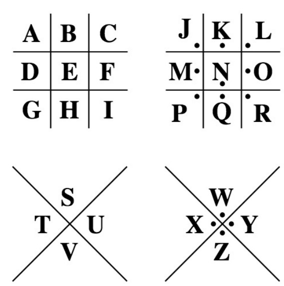
MATH/CSCI 408 Name: ______________________

CRYPTOGRAPHY MISSION 02 SOLUTIONS

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

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.

 (from `https://cryptii.com/text/pigpen`)

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

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

VGXUGEZA

   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:

The Transposition Cipher changes the orders of the letters in a plaintext phrase. In the example, it reverses the order of the letters.

   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).

Type some Sage code below and press Evaluate.

```
S = AlphabeticStrings()
E = TranspositionCryptosystem(S,14)
K = [14-i for i in range(14)]
e = E(K)
e(S("BABOUTHEOCELOT"))
```

Evaluate

```
TOLECOEHTUOBAB
```

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.

Note that we have

Plaintext	Vector	Plaintext	Vector
`so`	(18,14)	`GE`	(6,4)
`lv`	(11,21)	`ZX`	(25,23)
`ed`	(4,3)	`DS`	(3,18)

If we choose the last two pairs to set up an encryption matrix, we won't have a problem with finding an inverse.

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the encryption matrix. We know that to encrypt, we'd have

$$\begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix}$$

so to solve for M, we need

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 11 & 21 \\ 4 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \\ &= \frac{-1}{51} \begin{pmatrix} 3 & -21 \\ -4 & 11 \end{pmatrix} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \\ &= 25(25) \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \\ &= (1) \begin{pmatrix} 3 & 5 \\ 22 & 11 \end{pmatrix} \begin{pmatrix} 25 & 23 \\ 3 & 18 \end{pmatrix} \\ &\equiv \begin{pmatrix} 12 & 3 \\ 11 & 2 \end{pmatrix} \bmod 26 \end{aligned}$$

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.

We know that to encrypt, we'd have

$$\begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix}$$

so to solve for M, we need

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 3 & 14 \\ 13 & 19 \end{pmatrix}^{-1} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \\ &= \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 8 \end{pmatrix} \\ &\equiv \begin{pmatrix} 10 & 9 \\ 13 & 23 \end{pmatrix} \bmod 26 \end{aligned}$$

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.

The input is the same, but the output has changed. Now we have

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 9 & 18 \\ 13 & 11 \end{pmatrix} \begin{pmatrix} 4 & 11 \\ 13 & 10 \end{pmatrix} \\ &\equiv \begin{pmatrix} 10 & 19 \\ 13 & 19 \end{pmatrix} \bmod 26 \end{aligned}$$