CRYPTOGRAPHY MISSION 01 SOLUTIONS

Deadline: Thursday, 1 September 2016 at 3:05pm
This mission covers Sections 2.1, 2.2, and 2.3.

1. Graded Problems

1. Do the following survey: `http://tinyurl.com/16AnneHoSurvey`

2. (T&W 2.13 # 4) Consider an affine cipher (mod26). You do a chosen plaintext attack using `hahaha`. The ciphertext is `NONONO`. Determine the encryption function.

> Notice that we can set up ordered pairs with plaintext and ciphertext, so our pairs are `(h,N) and (a,O)`, which can be translated into (7,13) and (0,14). We want to find the line containing both. The slope is
>
> $$m = \frac{14-13}{0-7} = -\frac{1}{7} = -1(7^{-1}) = 25(15) \bmod 26 = 11 \bmod 26.$$
>
> The general affine encryption function is $f(x) = ax + b$ or $x \mapsto ax + b (\text{mod} 26)$. Here, we have $x \mapsto 11x + b$, so solving for b using one of our points, we get 1 mod 26, and our answer is $x \mapsto 11x + 14$.

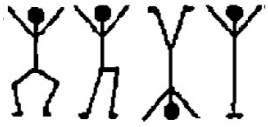
3. This problem involves the Dancing Men code from a Sherlock Holmes story.
   a. Read Section 2.5 (Sherlock Holmes), and describe (in a paragraph) how Sherlock figures out which dancing man represents the letter `e` as well as the letter `r`.

> Holmes first observes what the flags mean. Then he realizes that the most frequent symbol is likely `e`. Since the English language only has so many words with the structure `-e-e-` (including words like lever, never, or sever), he could use partial information to conclude that the last letter must be `r`.

   b. Explain in one sentence what the little flags mean.

> The flags denote the ends of words.

   c. Draw the dancing men figures that would correspond to the plaintext: `math`.



4. (T&W 2.14 # 2) The following ciphertext was the output of a shift cipher:

`LCLLEWLJAZLNNZMVYIYLHRMHZA`

By performing a frequency count, guess the key used in the cipher. What is the decrypted plaintext?

> `L` shows up 6 times, `Z` shows up 3 times, `A,H,M,N,Y` show up twice, and `C,E,I,J,R,V,W` show up once. Since the most common letter in the English alphabet is `e`, then we assume that the shift was from `e` to `L`, meaning all letters shifted by 6. This helps us translate the rest of the ciphertext to the plaintext: `eve expects eggs for breakfast`.

5. SageMathCloud:

   a. Set up a SageMathCloud account (`https://cloud.sagemath.com`). Create a new project (Cryptography). You can use this project folder to hold all of your SageMath code.

   b. From Moodle (`https://moodle.coastal.edu/`), download Dr. Ho's Vigenere cipher code (Vigenere Cipher.sagews) and upload it to your SageMathCloud project folder.

   c. Run through the cells of code, and then encode the phrase, "Hey, Mr. Tambourine Man, play a song for me" by using the key word "DYLAN". Write down the ciphertext. Be sure to print your code or email it to Dr. Ho too.

> One version of SageMath code is below:
>
> Type some Sage code below and press Evaluate.
>
> ```
> 2  Purpose: To encode a message for Mission 01 Problem 5.
> 3  Inputs:
> 4      - plaintext = text to encode
> 5      - key = keyword
> 6  Output:
> 7      - encrypted text
> 8  '''
> 9
> 10 alphabet = AlphabeticStrings()
> 11 plaintext = alphabet.encoding("Hey, Mr. Tambourine Man, play a song for me") #Inputs the text.
> 12 system = VigenereCryptosystem(alphabet,5) #The number here denotes the length of the key word.
> 13 key = alphabet("DYLAN") #Inputs a key word.
> 14 ciphertext = system.enciphering(key, plaintext) #Encrypts message.
> 15 ciphertext #Displays encrypted message.
> ```
>
> Evaluate
>
> ```
> KCJMEWYXBBXPTNRPYYPYDWLSBQEQOEPC
> ```