Homework 1

Due: Lesson 8

(50 pts)

Help Policy

AUTHORIZED RESOURCES: Any, except another cadet's program.

NOTE:

- Never copy another person's work and submit it as your own.
- Do not jointly create a program.
- You must document all help received from sources other than your instructor or instructor-provided course materials (including your textbook).
- **DFCS will recommend a course grade of F for any cadet who egregiously violates this Help Policy or contributes to a violation by others.**

1. [5] The ciphertext "YXCYIS" was produced by an affine cipher mod 26. You have reason to believe plaintext starts with "cr".

    a. What's the key?
    b. Decrypt the entire message.
    c. What kind of attack is this?

2. [5] Suppose we encrypt a message with an affine cipher using key K1, then encrypt the ciphertext with an affine cipher using key K2. Is this double encryption more secure than just doing a single encryption? Support your answer mathematically.

3. [5] Suppose our alphabet has only 3 letters, A, B, and C, which occur in plaintext with frequency 75%, 15%, 10%, respectively. A message is encrypted with a Vigenère cipher (mod 3, of course), using a key that is of length 1, 2, or 3 (you don't know which). If the ciphertext is CBCABAAACA.

    a. What is the most likely key length? Why?
    b. What is the likely key?

4. [5] A friend claims the following: The Vigenère cipher can be made stronger against cryptanalysis if one uses multiple rounds. That is, if a plaintext is encrypted with the Vigenère cipher with a key of length m, and the resulting ciphertext is again encrypted with the Vigenère cipher with a key of length n, then the net effect is the same as encryption with the Vigenère cipher with a longer key of length $m \cdot n$. In particular, your friend claims this is true only when m and n are relatively prime.

    a. Is your friend correct?

b. Why or why not?

5. [5] Let E_1 and E_2 be two independent tosses of a fair coin. Find the entropy $H(E_1)$ and joint entropy $H(E_1,E_2)$. Why is $H(E_1,E_2)=H(E_1)+H(E_2)$?

6. [5] Can you change the experiment in 5 (above) so that $H(E_1,E_2) < H(E_1)+H(E_2)$? Can you change it so $H(E_1,E_2) > H(E_1)+H(E_2)$?

7. [5] Let X be a random variable that takes on integer values. The probability is ½ that X will be in the range $[0,2^7-1]$ with all values in that range being equally likely. The rest of the time, it will be in the range $[2^7,2^{14}-1]$, again with uniform probability. What is the entropy H(X)? (Estimation is OK).

8. [5] A bag contains 6 red balls, 2 white balls, and 2 black balls.

   a. You choose 2 balls from the bag with replacement (i.e. you put the first ball back in and shake before drawing the second). What is the entropy of the experiment?

   b. You choose 2 balls from the bag without replacement (i.e. you keep the first ball while drawing the second). How is your uncertainty affected now that you know the color of the first ball before drawing the second? What is the entropy of this new experiment given the first ball you choose is red?

9. [10] Write a small program that loads in a text file of any size and then prints the frequency (as a percentage) of each character ('a'..'z'). All characters should be made lowercase for counting purposes. Ignore punctuation, spaces, etc. Output should be printed out by expected frequency order (e, t, a, o, etc.) and look something like:

```
'e' – 13.27%
't' – 9.11%
'a' – 8.47%
'o' – 7.32%
…
'q' – 0.01%
'z' – 0.00%
```

   Attach a printout of your code to your submission. Also, attach a printout of your code applied to THIS HANDOUT (ie: submit a screenshot of your results after analyzing the HW1 document). You may want to copy/paste the contents of this file into Notepad to create a text file your program can read.