**Homework 1 – Jacob Orner – T2A**

1. [5] The ciphertext “ADSSP” was produced by an affine cipher mod 26. You have reason to believe plaintext starts with “ha”.

a. What’s the key? α=15,

b. Decrypt the entire message. harry

c. What kind of attack is this? This is a known plaintext attack as we know the ciphertext and two letters of the plaintext.

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.

Assuming that K1 and K2 are different, then yes the double encryption would be more secure than a single encryption. With a single encryption, the ciphertext would be *x =* α*x* + . However, with double encryption, the ciphertext would be *x =* α2(α1*x* + β1 ) + β2, or *x =* α2α1*x* + α2β1 + β2. This mathematical operation of finding the plaintext is more difficult in the case of double encryption as there are four variables which must be found instead of two. Also, through the multiplication of α1 and β1 with α2 the encryption is more secure as there are two sets of variable to be found, and the must be found in order.

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 ABCBABBBAC.

a. What is the most likely key length? Why? The most likely key length is two, as when the key is compared to itself while displaced; a displacement of two had the most coincidences.

b. What is the likely key? The likely key is AC.

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∙n*. In particular, your friend claims this is true only when *m* and *n* are relatively prime.

a. Is your friend correct? No he is incorrect in his statement.

b. Why or why not? He is not correct as although the ciphertext would be thought to be more secure, if frequency analysis is used on the ciphertext, the most common letters used in the alphabet would still be visible through this process, and thus the key length and key could be found.

5. [5] Let E1 and E2 be two independent tosses of a fair coin. Find the entropy H(E1) and joint entropy H(E1,E2). Why is H(E1,E2)=H(E1)+H(E2)?

The entropy of E1 is 1 bit. The joint entropy of E1 and E2 is 2 bits. H(E1,E2)=H(E1)+H(E2) because the joint entropy is the sum of the entropy of each independent variable, and given the H(E1) = 1, then H(E1,E2) = 2.

6. [5] Can you change the experiment in 5 (above) so that H(E1,E2) < H(E1)+H(E2) ? Can you change it so H(E1,E2) > H(E1)+H(E2) ?

Yes, if X and Y are dependent, then H(E­1,E2) < H(E1) + H(E2) is possible. However, H(E1,E2) > H(E1)+H(E2) is not possible as H(E1,E2) is the sum of the individual entropies, and the sum of individual entropies cannot be greater than itself.

7. [5] Let X be a random variable that takes on integer values. The probability is ½ that X will be in the range with all values in that range being equally likely. The rest of the time, it will be in the range [26,215-1], again with uniform probability. What is the entropy H(X)? (Estimation is OK).

The entropy is 10.5 bits.

8. [5] A bag contains 6 red balls, 2 green 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?

H(x) = 1.37 bits.

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?

The uncertainty is diminished if the ball is green or black, as entropy drops to 1.22 bits. If the chosen ball is red, then the entropy of the new experiment is 1.44 bits.

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 sorted in decreasing 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.



