CSE 5351 Homework 1

Due: Thursday, January 25 by class time

1. Consider Caesar's shift cipher: $M = K = C = \{0, 1, 2, \ldots, 25\}$ and $\text{Enc}_k(m) = (m + k) \bmod 26$. Suppose $\Pr[\mathsf{M} = m] = (m+1)/S$ and $\Pr[\mathsf{K} = k] = (k+1)/S$ for all $m \in M$ and $k \in K$, where $S = 1 + 2 + 3 + \cdots + 26 = 351$. What is the probability of $\Pr[\mathsf{C} = 0]$? You may give your final answer as a summation of numbers (instead of a single value).

2. Assume Eve knows that Bob's password is either **abcd** or **bedg**. Suppose Bob encrypts his password using Caesar's shift cipher and Eve sees the resulting ciphertext. Show how Eve can determine Bob's password, or explain why this is not possible.

3. Repeat Question 2 for Vigenère cipher using period 2, using period 3, and using period 4. Assume Eve knows the period used. (period = key length.)

4. When using the one-time pad (Vernam's cipher) with the key $k = 0^n$, it follows that $\text{Enc}_k(m) = m \oplus k = m$ and the message is effectively sent in the clear! It has therefore been suggested to improve the one-time pad by only encrypting with a key $k \neq 0^n$ (i.e., to have Gen choose *k* uniformly at random from the set of *non-zero* keys of length *n*). **Question:** Is this an improvement? In particular, is the resulting scheme perfectly secret? Prove your answer.

5. Answer the following questions for the mono-alphabetic substitution cipher.
   a) Describe the key space *K*.
   b) Describe the largest message space $M \subseteq \{\text{a, b, …, z}\}^* = \bigcup_{i=1}^{\infty} \{\text{a, b, …, z}\}^i$ for which the mono-alphabetic substitution cipher provides perfect secrecy. (Note: a message is simply a string of letters; it doesn't have to be a "dictionary" word. For example, "abcxyz" can be a valid message.)