CSE 5351 Homework 1
Due: Wednesday, January 29 by class time

1. Consider the Caesar Cipher: \( M = K = C = \{0, 1, 2, \ldots, 25\} \) and \( \text{Enc}_k(m) = m + k \mod 26 \). Suppose \( \Pr(m) = (m + 1)/S \) and \( \Pr(k) = (k + 1)/S \) for all \( m \in M \) and \( k \in K \), where \( S = 1 + 2 + 3 + \cdots + 26 = 351 \). Derive the induced probability distribution over \( C \).

2. 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 \( \text{Gen} \) choose \( k \) uniformly at random from the set of non-zero keys of length \( n \)).

   **Question:** Is this an improvement? In particular, is it still perfectly secret? Prove your answer. If your answer is positive, explain why the one-time pad is not described in this way. If your answer is negative, reconcile this fact with the fact that encrypting with \( k = 0^n \) doesn't change the plaintext.

3. Describe the largest plaintext space \( M \) 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. Hint: what’s the key space of the mono-alphabetic substitution cipher?)

4. Prove or refute: Every encryption scheme for which the size of the key space equals the size of the message space, and for which the key is chosen uniformly from the key space, is perfectly secret.

5. Show that Vernam’s one-time pad is absolutely single-ciphertext indistinguishable. That is, show that either of the conditions in the definition of absolute ciphertext-indistinguishability holds. It is easier to use the second condition than the first one. Note that you **cannot** answer the question by saying that “Vernam’s one-time pad is perfectly secret and therefore absolutely ciphertext-indistinguishable.”