CSE 5351 Homework 2
Due: Thursday, February 1 by class time

1. Consider Caesar’s shift cipher with $M = \{a,b,c,d\}$ represented as $\{0,1,2,3\}$.
   - Key generation: $k \leftarrow \{0,\ldots,25\}$.
   - Encryption: $\text{Enc}_k(m) = \begin{cases} (m + k) \mod 26 & \text{with probability 1/2} \\ (m + k + 5) \mod 26 & \text{with probability 1/2} \end{cases}$
   - Assume $\Pr[M=m] = (m+1)/10$.

Questions:
(a) Compute $\Pr[\text{Enc}_k(m) = 10]$ for each $m \in M$. (K is random.)
(b) Compute $\Pr[\text{Enc}_k(M) = 10]$. (Both K and M are random.)

2. Let $\Pi$ denote the Vigenere cipher where the message space consists of all 3-character strings (i.e., $M = \{a, \ldots, z\}^3$), and the key is generated by first choosing the period $t \leftarrow \{1, 2, 3\}$ and then letting the key be a uniform string of length $t$ (i.e., $k \leftarrow \{a, \ldots, z\}^t$ or $\{0, \ldots, 25\}^t$).
   So, the key space is $K = \{a, \ldots, z\} \cup \{a, \ldots, z\}^2 \cup \{a, \ldots, z\}^3$.

Question: Compute $Pr[K = k]$ for $k = a$, $k = ab$, and $k = abc$.

3. Consider the encryption scheme $\Pi$ in Question 2 and the experiment $\text{PrivK}^{\text{cav}}_{A, \Pi}$, where adversary $A$ is defined as follows: $A$ outputs two messages $m_0 = \text{aab}$ and $m_1 = \text{abb}$.
   When given a challenge ciphertext $c$, $A$ outputs 0 if the first two characters of $c$ are the same, and outputs 1 otherwise.

Questions:
(a) Suppose Bob chooses $b = 0$. For what keys $k$ will $A$ succeed (i.e., $A(m_0,m_1,\text{Enc}_k(m_0)) = 0$)?
(b) Suppose Bob chooses $b = 1$. For what keys $k$ will $A$ succeed (i.e., $A(m_0,m_1,\text{Enc}_k(m_1)) = 1$)?

(One more question on page 2)
4. **Question**: Compute $\Pr[\text{Priv}^{eav}_A(m_0, m_1) = 1]$ for the scheme and adversary in Question 3.

**Hint**: $Pr[\text{Priv}^{eav}_A(m_0, m_1) = 1]$

$$= \sum_{b \in \{0,1\}, k \in K} \Pr[b = b] \cdot \Pr[K = k] \cdot \Pr[A(m_0, m_1, Enc_k(m_b)) = b]$$

$$= \frac{1}{2} \cdot \sum_{k \in K} \Pr[K = k] \cdot \Pr[A(m_0, m_1, Enc_k(m_0)) = 0]$$

$$+ \frac{1}{2} \cdot \sum_{k \in K} \Pr[K = k] \cdot \Pr[A(m_0, m_1, Enc_k(m_1)) = 1]$$