CSE 5351 Homework 2

Due: Thursday, February 1 by class time

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

   Questions:

   (a) Compute $\Pr[Enc_{\mathsf{K}}(m) = 10]$ for each $m \in M$. (K is random.)

   (b) Compute $\Pr[Enc_{\mathsf{K}}(\mathsf{M}) = 10]$. (Both K and M are random.)

2. Let Π denote the Vigenere cipher where the message space consists of all 3-character strings (i.e., $M = \{\text{a, ..., z}\}^3$), and the key is generated by first choosing the period $t \leftarrow_u \{1,\ 2,\ 3\}$ and then letting the key be a uniform string of length t (i.e., $k \leftarrow_u \{\text{a}, \ \ldots, \ \text{z}\}^t$ or $\{0, \ \ldots, \ 25\}^t$).
   So, the key space is $K = \{\text{a}, \ \ldots, \ \text{z}\} \cup \{\text{a}, \ \ldots, \ \text{z}\}^2 \cup \{\text{a}, \ \ldots, \ \text{z}\}^3$.
   Question: Compute $\Pr[\mathsf{K} = k]$ for $k = \text{a}$, $k = \text{ab}$, and $k = \text{abc}$.

3. Consider the encryption scheme Π in Question 2 and the experiment $\text{PrivK}^{\text{eav}}_{A,\Pi}$, 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., $A(m_0, m_1, Enc_k(m_0)) = 0$)?
   (b) Suppose Bob chooses $b = 1$. For what keys k will A succeed (i.e., $A(m_0, m_1, Enc_k(m_1)) = 1$)?

(One more question on page 2)

4. **Question:** Compute $\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\,\Pi}(m_0,\ m_1)=1\right]$ for the scheme and adversary in Question 3.

Hint: $\Pr\left[\mathrm{PrivK}^{\mathrm{eav}}_{A,\,\Pi}(m_0,\ m_1)=1\right]$

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

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

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