Tutorial 1: Perfect Secrecy

Submission Guidelines All problems must be solved in class today. Searching on the internet for solutions is strictly discouraged.

1. The shift cipher (also called Caesar cipher) works as follows. The English alphabet is represented by numbers from 0 to 25 i.e., $\{A, B, \ldots, Z\}$ are mapped to $\{0, 1, \ldots, 25\}$ in the same order.

   Define $\mathscr{K} = \{0, 1, 2, \ldots, 25\}$, $\mathscr{M} = \mathscr{C} = \{0, 1, 2, \ldots, 25\}^*$
   $\mathsf{Gen}()$: $k \xleftarrow{\mathrm{U}} \mathscr{K}$
   $\mathsf{Enc}(k, \mathbf{m} = m_1 m_2 \cdots m_n)$: Set $c_i \leftarrow m_i + k \bmod 26$. Ciphertext is given by $\mathbf{c} = c_1 c_2 \cdots c_n$.
   $\mathsf{Dec}(k, \mathbf{c} = c_1 c_2 \cdots c_n)$: Recover message components as $m_i \leftarrow c_i - k \bmod 26$.

   (a) Is it perfectly secret?

   (b) Can you modify the description to make it perfectly secret?

2. Prove or refute: Every encryption scheme for which the size of the key space $\mathscr{K}$ equals the size of the message space $\mathscr{M}$ and for which the key is chosen uniformly from $\mathscr{K}$, is perfectly secret.

3. Let $\varepsilon < 1$ be a constant. An encryption scheme $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over $(\mathscr{K}, \mathscr{M}, \mathscr{C})$ is called ε-almost perfectly secret if for any distribution over $\mathscr{M}$, any $m \in \mathscr{M}$ and any $c \in \mathscr{C}$,

   $$|\Pr[\mathrm{M} = m | \mathrm{C} = c] - \Pr[\mathrm{M} = m]| < \varepsilon.$$

   Show that if $\mathcal{E}$ is an ε-almost perfectly secret encryption scheme, then $|\mathscr{K}| \geq (1 - \varepsilon)|\mathscr{M}|$.

4. Modify the one-time pad as follows. Let $\mathscr{K} \subseteq \{0, 1\}^\ell$ and the key generation be such that first a key $\tilde{k}$ is uniformly chosen from $\{0, 1\}^{\ell/2}$ and then the key is defined by $k = \tilde{k} \| \tilde{k}$ where $\|$ denotes concatenation. (In addition, define $\mathscr{M} = \mathscr{C} = \{0, 1\}^\ell$.) Is this scheme perfectly secure? Justify your answer.