EE 720: Introduction to Number Theory and Cryptography (Autumn 2025)

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 1: 20 points — Date: August 11, 2025

1. [5 points] Consider the Vigenère cipher where the adversary knows that the key length is 100 characters. Let $S = \{0, 1, 2, \ldots, 25\}$. The key generation algorithm Gen generates the key $\mathbf{k} = k_0 k_1 k_2 \cdots k_{99}$ uniformly from the set S^{100}.

   Let $\mathcal{M} = \{0, 1, \ldots, 25\}^*$, i.e. the set of all finite length strings from the set $\{0, 1, \ldots, 25\}$. The encryption of a message $\mathbf{m} = m_0 m_1 \cdots m_{n-1} \in S^n$ is given by $\mathbf{c} = c_0 c_1 \cdots c_{n-1} \in S^n$ where $c_i = m_i + k_{i \bmod 100} \bmod 26$.

   Since the size of the key space is smaller than the size of the message space, this form of the Vigenère cipher is **not** perfectly secret. Then there must exist an adversary in the perfect indistinguishability experiment $\mathsf{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$ that succeeds with a probability greater than $\frac{1}{2}$. Find such an adversary $\mathcal{A}$.

2. [10 points] When using the one-time pad with the key $k = 0^l$, we have $\texttt{Enc}_k(m) = k \oplus m = m$ and the message is sent in the clear. It has therefore been suggested to modify the one-time pad by only encrypting with $k \neq 0^l$ (i.e., to have $\texttt{Gen}$ choose k uniformly from the set of nonzero keys of length l).

   Since the size of the key space is smaller than the size of the message space, this form of the one-time pad is **not** perfectly secret. Then there must exist an adversary in the perfect indistinguishability experiment $\mathsf{PrivK}^{\text{eav}}_{\mathcal{A},\Pi}$ that succeeds with a probability greater than $\frac{1}{2}$. Find such an adversary $\mathcal{A}$.

3. [5 points] For negligible functions negl_1 and negl_2, prove that $p_1(n)\mathsf{negl}_1(n) + p_2(n)\mathsf{negl}_2(n)$ is also negligible for any positive polynomials p_1, p_2.