EE 720: Introduction to Number Theory and Cryptography (Autumn 2024)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 1: 20 points | Date: August 16, 2024

---

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 $c_i = m_i + k_{i \bmod 100} \bmod 26$. Prove that this form of the Vigenère cipher is **not** perfectly secret.

2. [5 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). Is this modified scheme still perfectly secret? Explain.

3. [5 points] For a negligible function negl, prove that $p(n)\mathsf{negl}(n)$ is also negligible for any positive polynomial p.

4. [5 points] Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. **Prove or disprove** that the following functions are pseudorandom generators where $s \in \{0,1\}^n$ and s_i is the ith bit of s. The $\|$ denotes the string concatenation operator.

   (a) $G_1(s) = G(s)\|0$.

   (b) $G_2(s) = G(s_1, s_2, \ldots, s_{|s|-1})\|s_{|s|}$.

   (c) $G_3(s) = G(s\|0)$.