EE 720: Introduction to Number Theory and Cryptography (Spring 2019)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 10 points Date: January 23, 2019

Upload the solutions as a **pdf** file in Moodle. You can upload a scanned version of your handwritten solution. The **upload deadline** will be 11:00pm IST on Wednesday, January 30, 2019.

1. [2 points] State whether the following encryption scheme is perfectly secret or not. Justify your answer either with a proof or a counterexample.

   The message space is $\mathcal{M} = \{0, \ldots, 4\}$. Algorithm $\texttt{Gen}$ chooses a uniform key from the keyspace $\{0, \ldots, 5\}$. $\texttt{Enc}_k(m) = (k + m) \bmod 5$ and $\texttt{Dec}_k(c) = (c - k) \bmod 5$.

2. [2 points] Consider a variant of the one-time pad with message space $=\{0,1\}^l$ and keyspace $\mathcal{K}$ restricted to all l-bit strings with an even number of 1's. Is this scheme perfectly secret? Justify your answer either with a proof or a counterexample.

3. [2 points] Let $\texttt{negl}_1$ be a negligible function. Prove that for any positive polynomial p, the function $\texttt{negl}_2$ defined by $\texttt{negl}_2(n) = p(n) \cdot \texttt{negl}_1(n)$ is negligible.

4. [4 points] Let $G : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a pseudorandom generator with expansion factor $l(n) > n$. Assume that G is defined for all $n \geq 1$. Prove that G_1 defined below is a pseudorandom generator where $|s|$ denotes the length of s, $|s| \geq 2$, and s_i is the ith bit of s.

$$G_1(s) = G(s_1, s_2, \ldots, s_{|s|-1}) \| s_{|s|}.$$