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

Assignment 3: 10 points Date: February 3, 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 Sunday, February 10, 2019.

1. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a keyed pseudorandom permutation (the first argument is the key). Consider the keyed function $F' : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, x' \in \{0,1\}^n$ by

$$F'_k(x \| x') = F_k(x) \| F_k(x \oplus x').$$

   (a) [1 point] Prove that F'_k is a permutation for all $k \in \{0,1\}^n$.

   (b) [4 points] Prove that F'_k is **not** a pseudorandom permutation.

2. [5 points] Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation. Suppose messages of size dn bits have to be encrypted where $d > 1$. The message m is divided into d blocks of n bits each where m_i is the ith block. Consider the mode of operation in which a uniform value $\texttt{ctr} \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(\texttt{ctr} + i + m_i)$. The value $\texttt{ctr}$ is sent in the clear, i.e. the eavesdropper observes $\texttt{ctr}, c_1, c_2, c_3, \ldots, c_d$. The sum $\texttt{ctr} + i + m_i$ is calculated modulo 2^n ensuring that the argument of F_k belongs to $\{0,1\}^n$. Show that this scheme does **not** have indistinguishable encryptions in the presence of an eavesdropper.