EE 720: Introduction to Number Theory and Cryptography (Spring 2020)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 2: 10 points — Date: February 4, 2020

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 9, 2020.

1. [3 points] Consider the following private-key encryption scheme $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ where message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$ are both equal to $\{0,1\}^n$. Let the key space $\mathcal{K}$ be the set of all $n!$ permutations of the set $\{1, \dots, n\}$.

   - `Gen`: Choose k uniformly from $\mathcal{K}$. Let $k = (k_1, k_2, \dots, k_n)$. For example, if $n = 4$ then $k = (2, 1, 3, 4)$ is the permutation which swaps the positions of the first two elements.
   - `Enc`: For $m \in \{0,1\}^n$, let $m[i]$ denote the ith bit of m. Output the ciphertext $c \in \{0,1\}^n$ as
   $$c := (m[k_1], m[k_2], \dots, m[k_n]).$$
   - `Dec`: Given $k \in \mathcal{K}$ and ciphertext $c \in \{0,1\}^n$, output the message m by inverting the permutation.

   Prove that this scheme is **not EAV-secure**.

2. [3 points] Consider a linear feedback shift register (LFSR) which has n registers. Let the initial state of the LFSR be $s = (s_1, s_2, \dots, s_n)$ where each $s_i \in \{0,1\}$. Let the feedback equation be given by
$$s_{j+n+1} = \bigoplus_{i=1}^{n} a_i s_{j+i}$$
   where $a_i \in \{0,1\}$ and $j \geq 0$. Let $G : \{0,1\}^n \mapsto \{0,1\}^m$ be the output of the LFSR when restricted to m bits where $m > n$. So $G(s) = (s_1, s_2, \dots, s_m)$.

   Prove that G is **not a pseudorandom generator** irrespective of how the values of a_i are chosen.

3. [4 points] Let F be a length-preserving pseudorandom function having key length, input length, and output length all equal to n bits. Consider the following keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \mapsto \{0,1\}^{2n}$ defined as
$$F'_k(x) = F_k(0\|x)\|F_k(x\|1).$$
   Prove that the F' is **not** a pseudorandom function. Here $F'_k(x) = F'(k, x)$, $F_k(y) = F(k, y)$, and $\|$ is the string concatenation operator.