EE 720: Introduction to Number Theory and Cryptography (Autumn 2026)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Assignment 3: 20 points Date: September 7, 2026

1. Suppose $F : \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n$ is a length-preserving pseudorandom function. **Using only F, give constructions** of schemes which satisfy the following properties. You can use results discussed in class without proof.
   (a) [2 points] A CPA-secure encryption scheme for messages of length n which is not CCA-secure. Describe the algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.
   (b) [2 points] A CPA-secure encryption scheme for messages of length $3n$. Describe the algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.
   (c) [2 points] A secure MAC for messages of length $3n$. Describe the algorithms $(\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$.
   (d) [4 points] A CCA-secure encryption scheme for messages of length $3n$. Describe the algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$.

2. [10 points] Alice has a length-preserving pseudorandom function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. She wants to authenticate messages of length $2n$. Let $m \in \{0,1\}^{2n}$ denote the message. Let $m_1 \in \{0,1\}^n$ denote the first n bits of m and let $m_2 \in \{0,1\}^n$ denote the last n bits of m. Alice uses the MAC scheme $\Pi = (\mathtt{Gen}, \mathtt{Mac}, \mathtt{Vrfy})$ where:

   - `Gen`: Key k is chosen uniformly from $\{0,1\}^n$.
   - `Mac`: The message space $\mathcal{M} = \{0,1\}^{2n}$. Given key k, the tag corresponding to $m = (m_1, m_2) \in \{0,1\}^{2n}$ is given by a $2n$-bit string t as follows.
   $$\mathsf{Mac}_k(m) = t := \langle t_1, t_2 \rangle = \langle F_k(m_1), F_k(m_1 \oplus m_2) \rangle.$$
   - `Vrfy`: Given key k, message $m = (m_1, m_2)$ and tag $t = \langle t_1, t_2 \rangle$, the verifier recomputes the tag on the message
   $$t' := \langle t'_1, t'_2 \rangle = \langle F_k(m_1), F_k(m_1 \oplus m_2) \rangle.$$
   If $t = t'$, then the verifier outputs 1 and 0 otherwise.

   Prove that Alice's MAC scheme is **not** secure.