Fundamentals of Information Science: Homework 9

May 14, 2025

Problem 1. multiplicative one-time pad
We may also define a "multiplication mod p" variation of the one-time pad. This is a cipher $\mathcal{E} = (E, D)$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{1, ..., p-1\}$, where p is a prime. Encryption and decryption are defined as follows:

$$E(k, m) := k \cdot m \mod p \quad D(k, c) := k^{-1} \cdot c \mod p.$$

Here, k^{-1} denotes the multiplicative inverse of k modulo p. Verify the correctness property for this cipher and prove that it is perfectly secure.

Problem 2. Truncating PRFs
Let F be a PRF whose range is $\mathcal{Y} = \{0, 1\}^n$. For some $\ell < n$ consider the PRF F' with a range $\mathcal{Y}' = \{0, 1\}^\ell$ defined as: $F'(k, x) = F(k, x)[0...\ell]$. That is, we truncate the output of $F(k, x)$ to the first ℓ bits. Show that if F is a secure PRF then so is F'.

Problem 3. Chain encryption
Let $\mathcal{E} = (E, D)$ be a perfectly secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{K} = \mathcal{M}$. Let $\mathcal{E}' = (E', D')$ be a cipher where encryption is defined as $E'((k_1, k_2), m) := (E(k_1, k_2), E(k_2, m))$. Show that $\mathcal{E}'$ is perfectly secure.