Introduction to Cryptology ENEE459E/CMSC498R: Homework 3

Due by beginning of class on 4/8/2014.

1. Exercise 4.1

2. Exercise 4.2

3. Exercise 4.3

4. Exercise 4.4

5. Let F be a pseudorandom function. Show that each of the following message authentication codes is insecure. (In each case the shared key is a random $k \in \{0,1\}^n$.)

   (a) To authenticate a message $m = m_1||\cdots||m_\ell$, where $m_i \in \{0,1\}^n$, compute $t := F_k(m_1 \oplus \cdots \oplus m_\ell)$.

   (b) To authenticate a message $m = m_1||m_2$, where $m_1, m_2 \in \{0,1\}^n$, compute $t := F_k(m_1)||F_k(m_2 \oplus F_k(m_1))$.

   (c) To authenticate a message $m = m_1||m_2$, where $m_1, m_2 \in \{0,1\}^n$, compute $t := F_k(m_1 \oplus m_2)||F_k(m_2 \oplus F_k(m_1))$.

   (d) To authenticate a message $m = m_1||\cdots||m_\ell$, where $m_i \in \{0,1\}^n$, choose $r \in \{0,1\}^n$ at random and compute $t := r||F_k(m_1 \oplus r)||\cdots||F_k(m_\ell \oplus r)$.