Cryptography: Homework 9
(Deadline: Nov 29, 2018)

1. (20 points) Determine whether the following encryption schemes are IND-CPA secure.

   (a) Fix $IV = 0^n$ in the CBC mode of encryption.

   (b) Let F be a length-preserving PRP ($|k| = |x| = |F_k(x)|$). Let $\langle i \rangle$ be the n-bit representation of any integer $0 \leq i < 2^n$. In order to encrypt any message $m = m_1 m_2 \cdots m_t$, where $m_i \in \{0,1\}^n$ for every i, choose a uniform value $\text{ctr} \leftarrow \{0,1\}^n$, compute $c_i = F_k(\text{ctr} \oplus \langle i \rangle \oplus m_i)$ for all i, and output the ciphertext $c = (\text{ctr}, c_1, \ldots, c_t)$.

2. (30 points) Let F be a pseudorandom function. Show that each of the following MACs is not EUF-CMA. (Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.)

   (a) A fixed-length MAC that authenticates messages of $3n/2$ bits.

   - $\mathsf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$ uniformly as the secret key.
   - $\mathsf{Mac}(k, m)$: To authenticate a message $m = m_1 m_2 m_3$, where $m_i \in \{0,1\}^{n/2}$ for every $i \in \{1,2,3\}$, compute and output the tag

   $$t = F_k(\langle 1 \rangle \| m_1) \oplus F_k(\langle 2 \rangle \| m_2) \oplus F_k(\langle 3 \rangle \| m_3).$$

   - $\mathsf{Vrfy}(k, m, t)$: for a message $m = m_1 m_2 m_3 \in \{0,1\}^{3n/2}$ and a tag $t \in \{0,1\}^n$, output 1 if and only if $t = F_k(\langle 1 \rangle \| m_1) \oplus F_k(\langle 2 \rangle \| m_2) \oplus F_k(\langle 3 \rangle \| m_3)$.

   (b) A fixed-length MAC that authenticates messages of $n/2$ bits.

   - $\mathsf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$ uniformly as the secret key.
   - $\mathsf{Mac}(k, m)$: To authenticate a message $m \in \{0,1\}^{n/2}$, choose $r \leftarrow \{0,1\}^n$ uniformly, compute $s = F_k(r) \oplus F_k(\langle 1 \rangle \| m)$, output the tag $t = (r, s)$.
   - $\mathsf{Vrfy}(k, m, t)$: for a message $m \in \{0,1\}^{n/2}$ and a tag $t = (r, s)$, output 1 if and only if $s = F_k(r) \oplus F_k(\langle 1 \rangle \| m)$.