Cryptography: Homework 6

(Deadline: 11:59am, 2019/11/6)

1. (40 points) Determine if the following modifications on the modes of encryption result in IND-CPA secure schemes. Prove your answers.

   (a) In the OFB-mode encryption fix the initialization vector as $IV = 0^n$.

   (b) In the CBC-mode encryption fix the initialization vector as $IV = 0^n$.

   (c) Make the CBC-mode encryption **stateful** such that the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time).

   (d) In the CTR-mode encryption compute each ciphertext block c_i as $c_i = F_k(\text{ctr} \oplus \langle i \rangle \oplus m_i)$, where F is a PRP and $\langle i \rangle \in \{0,1\}^n$ is the n-bit binary representation of i.

2. (20 points) Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be a length-preserving PRF. Define a MAC $\Pi = (\mathbf{Gen}, \mathbf{Mac}, \mathbf{Vrfy})$ for messages of length n as below:

   - $\mathbf{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$;
   - $\mathbf{Mac}(k, m)$: for $m \in \{0,1\}^n$, output $t = F_k(m) \in \{0,1\}^n$.
   - $\mathbf{Vrfy}(k, m, t)$: output 1 if $t = F_k(m)$ or $t = F_k(m) \oplus 1^n$.

   Determine if Π is EUF-CMA secure or strong EUF-CMA secure. Prove your answers.