Problem 5): The **ECB** mode of operation is defined, it terms of the expression for the resulting cipher-text c, according to

$$c = \{F_k(m_1), F_k(m_2), \ldots, F_k(m_i), \ldots, F_k(m_l)\} \tag{5.1}$$

where $F_k(m_i)$ is a pseudo random permutation function with key k and the m_i are the blocks of the message. Since each block is directly encrypted by $F_k(m_i)$, any $m_i \in \mathcal{M}$ can result in only one unique $c_i \in \mathcal{C}$ when passed to $F_k(m_i)$ this mode is deterministic and therefore *not* **CPA** secure. Since this mode is not **CPA** secure, it *cannot* be *CCA* secure. This is follows from the fact that *CCA* security of an encryption scheme $\prod$ implies the *CPA* security of $\prod$.

We also define the **CTR** mode of operation in terms of the expression for resulting cipher-text c. For this mode of operation we have

$$c = \{c_0, c_1, c_2, \ldots, c_i, \ldots, c_l\} \tag{5.2}$$

with $c_0 = \texttt{ctr}$ and the remaining c_i defined as $c_i = r_i \oplus m_i$. Here the m_i are the blocks of the message and the r_i are defined, in terms of their index i, some random initial counter value `ctr`, and the keyed pseudo random permutation function $F_k(r_i)$, according to

$$r_i = F_k(\texttt{ctr} + i) \tag{5.3}$$

Since $r_i = F_k(\texttt{ctr} + i)$ and `ctr` is chosen at random, the set of all r_i, $r = \{r_1, r_2, \ldots, r_i, \ldots, r_l\}$ represents a pseudo random sequence with the same length as the message. This implies that result $c_i = r_i \oplus m_i$ for each block of the message m_i depends on both on m_i and r_i instead of only m_i and the keyed pseudo random permutation function $F(m_i)$. By extension, any arbitrary message $m \in \mathcal{M}$ can be encrypted into any cipher-text $c \in \mathcal{C}$ with some non-zero probability, thereby making the **CTR** mode of operation probabilistic and thus **CPA** secure. Since the first block of the message, c_0, holds the value of `ctr` in the clear, the cipher-text resulting from this mode of operation is deterministic on the value of `ctr`.

This enables an adversary to employ a **CCA** attack by sending $m_0 = 0^n$ and $m_1 = 1^n$ to the encryption oracle, flipping the first bit of c_1 in the cipher-text c returned by the encryption oracle to obtain c', and then sending c' to the decryption oracle to obtain either 10^{n-1} or 01^{n-1}. The possible results from the decryption oracle respectively imply that either m_0 was enciphered to into c or m_1 was enciphered into c thus giving the adversary two messages, cipher-text associated with each message, and the value of `ctr` used for encrypting both message. This information allows the adversary to eventually to recover the pseudo random permutation function F_k and its associated key used in to encrypt these messages. This attack is made possible because only the first bit in the cipher-text for m was changed and this first block of cipher-text is *directly* dependent on only the corresponding message block m_1 and the key k when the the value of `ctr` is known. The **CCA** attack exploits the fact that encryption in **CTR** mode becomes deterministic the on the values of `ctr` and some cipher-text are known.