Cryptography: Homework 5

(Deadline: 10am, 2022/10/28)

1. (20 points) Determine if the following modifications on the modes of operation result in CPA-secure schemes. Explain your answers.

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

   (b) 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. (30 points) Let F be a PRF and G be a PRG with expansion factor $\ell(n) = n + 1$. For each of the following encryption schemes, state whether the scheme is EAV-secure and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answers.

   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose $r \in \{0,1\}^n$ uniformly and output $c = (r, G(r) \oplus m)$.

   (b) To encrypt $m \in \{0,1\}^n$, output $c = m \oplus F_k(0^n)$.

   (c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose $r \in \{0,1\}^n$ uniformly and output $c = \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.