CSE 5351 Homework 3

Due: Tuesday, February 13 by class time

1. Let G be a pseudorandom generator with expansion factor $\ell(n) = 2n.$ Define $F(k,x) = G(k) \oplus x$ for $k \in \{0,1\}^n$ and $x \in \{0,1\}^{2n}$ (thus, $F_k(x) = G(k) \oplus x$)
(Note: here $\ell_{\text{key}}(n) = n,\ \ell_{\text{in}}(n) = \ell_{\text{out}}(n) = 2n.$) Question: Is F a pseudorandom function? That is, is the following true? Justify your answer.

$$\Big|\ \Pr\left[D^{F_k(\cdot)}(1^n) = 1:\ k \leftarrow_u \{0,1\}^n\right] - \Pr\left[D^{f(\cdot)}(1^n) = 1:\ f \leftarrow_u \text{Func}_{2n}\right]\Big| \le \text{negl}(n)$$

where Func_{2n} is the set of all functions $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$.

2. Let F be a (length-preserving) pseudorandom function and G a pseudorandom generator 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 key is a uniform $k \in \{0,1\}^n$.) Explain your answer.

   (a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and let $c := \langle r,\ G(r) \oplus m \rangle$.

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

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

3. Say CBC- mode is used with a block cipher having a 256-bit key and 128-bit block length to encrypt a 1024-bit message. What is the length of the resulting ciphertext? (Assume a padding scheme that appends to the message a 1 and as many 0's as needed.)