1. Let \( F : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^* \) be a pseudorandom function. For all \( sk \in \{0, 1\}^n \) and for all input \( x \in \{0, 1\}^n \), define \( F'_{sk}(x) := F_{sk}(x) || F_{sk}(x + 1) \). Is \( F' \) a pseudorandom function? If yes, prove it; if not, show an attack.

2. Let \( F \) be a length-preserving pseudorandom function. For the following constructions of a keyed function \( F' : \{0, 1\}^n \times \{0, 1\}^{n-1} \rightarrow \{0, 1\}^{2n} \), state whether \( F' \) is a pseudorandom function. If yes, prove it; if not, show an attack.
   
   (a) \( F'_k(x) := F_k(0 || x) || F_k(1 || x) \).
   
   (b) \( F'_k(x) := F_k(0 || x) || F_k(x || 1) \).

3. Consider the following keyed function \( F \): For security parameter \( n \), the key is an \( n \times n \) Boolean matrix \( A \) and an \( n \)-bit Boolean vector \( b \). Define \( F_{A,b} : \{0, 1\}^n \rightarrow \{0, 1\}^n \) by \( F_{A,b} := Ax + b \), where all operations are done modulo 2. Show that \( F \) is not a pseudorandom function.

4. Let \( F \) be a pseudorandom function and \( G \) be a pseudorandom generator with expansion factor \( \ell(n) = n + 1 \). For each of the following encryption schemes, state whether the scheme has indistinguishable encryptions in the presence of an eavesdropper and whether it is CPA-secure. (In each case, the shared 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 output the ciphertext \( \langle r, G(r) \oplus m \rangle \).
   
   (b) To encrypt \( m \in \{0, 1\}^n \), output the ciphertext \( m \oplus F_k(0^n) \).
   
   (c) To encrypt \( m \in \{0, 1\}^{2n} \), parse \( m \) as \( m_1 || m_2 \) with \( |m_1| = |m_2| \), then choose uniform \( r \in \{0, 1\}^n \) and send \( \langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r + 1) \rangle \).

5. What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext \( c_1, c_2, c_3, \ldots \) is received as \( c_1, c_3, \ldots \)) when using the CBC, OFB, and CTR modes of operation?