Question 1:
Let $F$ be a length-preserving pseudorandom function. For the following construction 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.

1. $F'_k(x) = F_k(0||x)\|F_k(1||x)$.
2. $F'_k(x) = F_k(0||x)\|F_k(x||1)$.

Question 2:
Prove that if $F$ is length-preserving pseudorandom function, then $G(s) = F_s(1)||F_s(2)||\ldots||F_s(\ell)$ is a pseudorandom generator with expansion factor $\ell \cdot n$.

Question 3:
What is the effect of a single bit of error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

Question 4: (Robust combiners)
1. You have two candidates for pseudorandom generator from $n$ to $4n$ bits, $G_1$ and $G_2$ in which only one of the two is secure (you do not know which one). Using $G_1$ and $G_2$, show how to construct a pseudorandom generate $G$ from $n$ to $2n$ bits. Provide a full proof of your solution.
2. Let $\Pi_1 = (Gen_1, Enc_1, Dec_1)$ and $\Pi_2 = (Gen_2, Enc_2, Dec_2)$ be two encryption schemes for which it is known that at least one is CPA-secure (but you do not know which one). Show ho to construct an encryption scheme $\Pi$ that is guaranteed to be CPA-secure as long as at least one of $\Pi_1$ or $\Pi_2$ is CPA-secure. Provide a full proof of your solution.

Question 5: Let $F$ be a pseudorandom function. Show that the following MAC for messages of length $2n$ is insecure: $Gen$ outputs a uniform $k \in \{0,1\}^n$. To authenticate a message $m_1||m_2$ with $|m_1| = |m_2| = n$, compute the tag $F_k(m_1)\|F_k(F_k(m_2))$.

Question 6: Show that appending the message length to the end of the message before applying basic CBC-MAC does not result in a secure MAC for arbitrary-length messages.