Question 1

Let \((\text{Enc}, \text{Dec})\) be a (deterministic) encryption scheme with key length \(k\) and message length \(m\). Suppose that \(\text{Enc}(K, M)\) and \(\text{Enc}(K, M')\) are \(\frac{1}{2}\)-statistically close for every two messages \(M, M'\).

(a) Show that \(\text{Enc}(K, M')\) is a possible encryption of \(M\) with probability more than \(\frac{1}{2}\).

(b) Fix a message \(M\). Show that there exists a key \(K\) for which \(\text{Enc}(K, M')\) is a possible encryption of \(M\) for more than half the messages \(M'\).

(c) Show that if \(m > k\) then \((\text{Enc}, \text{Dec})\) is not an encryption scheme.

Question 2

In Lecture 2 we showed that if \(G: \{0, 1\}^k \rightarrow \{0, 1\}^n\) is an \((s, \varepsilon)\)-pseudorandom generator of size \(t\) then

\[
G'(K) = (\text{first } n - k \text{ bits of } G(K), G(\text{last } k \text{ bits of } G(K)))
\]

is an \((s - t, 2\varepsilon)\)-pseudorandom generator. Assuming that pseudorandom generators (with sufficiently good parameters) exist, show that there is a \(G: \{0, 1\}^k \rightarrow \{0, 1\}^n\) that is an \((s, \varepsilon)\)-pseudorandom generator but such that \(G'\) is not a \((\omega(n), 1.99\varepsilon)\)-pseudorandom generator.

Question 3

Let \(F_K\) be a pseudorandom function. Are these functions also pseudorandom? Assume the key length, input length, and output length are all equal to the security parameter \(k\).

(a) The function \(F'_K(x) = F_K(F_K(x))\).

(b) The function \(F'_{K,K'}(x, y) = F_K(x) + F_{K'}(y)\), where \(K\) and \(K'\) are independent.

(c) \((\text{Optional})\) The function \(F'_K(x) = F_K(x + K)\).

If you answer yes, you need to give a proof that \(F'\) is pseudorandom if \(F\) is, namely prove that if \(F'\) has an efficient distinguisher so does \(F\). Try to work out the best parameters you can.

If you answer no, you need to give a pair of functions \(F, F'\) such that \(F\) is pseudorandom but \(F'\) is not (assuming pseudorandom functions exist).
Question 4

In our setup of private-key encryption we assumed that Alice and Bob share identical copies of the random key. Now suppose that Alice’s and Bob’s copies of the key are noisy. Specifically, the keys $K_A, K_B$ are elements of the group $\mathbb{Z}_{2^k}$ (i.e., integers modulo $2^k$) that are individually uniformly distributed such that the difference $K_A - K_B$ is in the range from $-2^b + 1$ to $2^b$ modulo $2^k$ (where $b < k$).

(a) Give a definition of a noisy key encryption scheme.

(b) Show that if the message length is less than $k - b$ then there exists a perfectly secure noisy key encryption scheme.

(c) Show that if the message length is $k - b$ or more then perfect security is no longer possible. Show how to construct a message-simulatable (computationally secure) scheme assuming the existence of a pseudorandom generator. Provide a proof of security.