Problem 1

Suppose (Enc, Dec) is a private key encryption scheme with key length k and message length m with $k < m$. Show that there exist a pair of messages (M, M') and a function $A\colon \{0,1\}^m \to \{0,1\}$ such that

$$\Pr_{K\sim\{0,1\}^k}[A(Enc(K, M)) = 1] - \Pr_{K\sim\{0,1\}^k}[A(Enc(K, M')) = 1] > 1/2.$$

Problem 2

Let $G\colon \{0,1\}^k \to \{0,1\}^{3k}$ be a pseudorandom generator. Are these functions also pseudorandom generators?

(a) $G'\colon \{0,1\}^{2k} \to \{0,1\}^{3k}$ given by $G'(x, x') = G(x) + G(x')$

(b) $G'\colon \{0,1\}^k \to \{0,1\}^{4k}$ given by $G'(x) = (x, G(x)) + (G(x), x)$.

Here x and x' are strings of length k. If you answer yes, give a proof that G' is pseudorandom assuming G is. If you answer no, you need to provide a pair of functions G, G' with proofs that G is pseudorandom but G' is not (assuming pseudorandom generators exist).

Problem 3

Let $F_K\colon \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Are these functions also pseudorandom?

(a) The function $G_K(x, y) = F_K(x) + F_K(y)$.

(b) The function $G_{K,K'}(x, y) = F_K(x) + F_{K'}(y)$, where $K, K' \sim \{0,1\}^k$ are independent random keys.

(c) **(Optional)** The function $G_K(x) = F_K(x + K)$.

If you answer yes, you need to give a proof that G is pseudorandom if F is, namely prove that if G has an efficient distinguisher so does F. If you answer no, you need to give a pair of functions F, G such that F is pseudorandom but G is not (assuming pseudorandom functions exist).

Problem 4

In our setup of private-key encryption we assumed that Alice and Bob share identical copies of the random key $K \in \{0,1\}^k$. Now suppose that Alice's and Bob's copies of the key are not exactly the same but they differ in one random bit (which Alice and Bob don't know). Formally, the pair of keys (K_A, K_B) is chosen from the following distribution on $\{0,1\}^k \times \{0,1\}^k$: First, choose K_A uniformly at random from $\{0,1\}^k$, then choose $i \in \{1,\ldots,k\}$ uniformly at random and flip the i-th bit of K_A to obtain K_B. Let's call this *noisy key encryption*.

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

(b) Assuming the existence of pseudorandom generators, prove the existence of a message indistinguishable noisy key encryption scheme.

(c) **(Optional)** Can you do part (b) in case K_A and K_B differ in $0.1k$ positions? What about $0.51k$?