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') such that

$$\Pr_{K \sim \{0,1\}^k}[Enc(K, M) \text{ is a possible ciphertext for } M'] < 1/2.$$

Problem 2

You want to design an encryption scheme that is perfectly secure (for a single message), but with an additional requirement: Even if Eve gets to inspect any one bit of the key (a bit she can choose), the scheme remains perfectly secure. Let's call this *perfectly secure encryption with one bit of leakage.*

(a) Give a definition of perfectly secure encryption with one bit of leakage.

(b) Give a perfectly secure encryption scheme with one bit of leakage for key length k and message length m, where $k = m + 1$.

(c) Show that if $k < m + 1$, there does not exist a perfectly secure encryption scheme with one bit of leakage for key length k and message length m.

(d) Can you generalize parts (b) and (c) if b bits of leakage are allowed?

Problem 3

Suppose you are given a pseudorandom generator $G\colon \{0,1\}^k \to \{0,1\}^{k+1}$ (assume k is even) and you want to construct another one that has more bits of output. Here is a candidate construction $G'\colon \{0,1\}^{3k/2} \to \{0,1\}^{2k+2}$:

$$G'(x_1x_2x_3) = G(x_1x_2), G(x_2x_3)$$

where $|x_1| = |x_2| = |x_3| = k/2$.

Show that this construction doesn't work. Specifically, assuming that pseudorandom generators exist, prove that there exists a G such that G is pseudorandom but G' is not.

Problem 4

Let $\mathcal{F} = \{F\colon \{0,1\}^n \to \{0,1\}^n\}$ be a family of functions where every $F \in \mathcal{F}$ can be evaluated by a circuit of size t.

(a) Show that if $\mathcal{F}$ is an (s, ε) pseudorandom function family, then for every oracle circuit A of size at most s/t,

$$|\Pr_{F,F'\sim\mathcal{F}}[A^{F,F'} = 1] - \Pr_{R,R'}[A^{R,R'} = 1]| \leq 2\varepsilon,$$

where R and R' are random functions from $\{0,1\}^n$ to $\{0,1\}^n$.

(b) (Optional) Is the following statement true or false?

Suppose for every s and every oracle circuit A of size s,

$$|\Pr_{F\sim\mathcal{F}}[A^F = 1] - \Pr_R[A^R = 1]| \leq \varepsilon(s).$$

(You can assume $\varepsilon(s)$ is nondecreasing.) Then for every oracle circuit B of size s/t,

$$|\Pr_{F,F'\sim\mathcal{F}}[B^{F,F'} = 1] - \Pr_{R,R'}[B^{R,R'} = 1]| \leq \max_{0\leq r\leq s}\{\varepsilon(s-r) + \varepsilon(r)\} + \mathrm{negl}(n)$$

where $\mathrm{negl}(n)$ is a negligible function.