Problem Set 1

1. Let $G : \{0,1\}^k \to \{0,1\}^m$ be a (t, ϵ)-secure pseudoradom generator.

   Prove that

   $$\frac{t}{\epsilon} \leq 2^k \cdot O(m)$$

2. Let $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$ be a (t, ϵ)-secure pseudorandom function with $k = m$.

   Prove that

   $$\frac{t}{\epsilon} \leq 2^k \cdot O(m)$$

3. Problem 3.7 in Katz-Lindell: assuming the existence of a CPA-secure cryptosystem (Enc, Dec), show that there is a cryptosystem (Enc', Dec') that satisfies plain security for multiple encryptions but that is not CPA secure.

   [Hint: insert a kind of "backdoor" in (Enc', Dec') which can be exploited in a CPA attack but that is exponentially unlikely to be exploitable in the plain multiple encryption model.]

4. Suppose that F is a pseudorandom permutation. Consider the following encryption scheme:

   - $Enc(K, M)$: pick a random string r, output $(F_K(r), r \oplus M)$
   - $Dec(K, C_0, C_1) := I_K(C_0) \oplus C_1$

   Is it CPA secure?