MATH 3540 **Name:** _____
Homework 4

Directions

1. Complete the following questions.

---

1. Let F be a pseudorandom function with 128-bit key and 256-bit block length. Which of the following functions G are necessarily pseudorandom generators?

   (a) $G(x) = F_x(0\ldots0)\|F_x(0\ldots0)$, where x is a 128-bit input.

   (b) $G(x) = F_x(0\ldots0)$, where x is a 128-bit input.

   (c) $G(x) = F_{0\ldots0}(x)\|F_{1\ldots1}(x)$, where x is a 256-bit input

   (d) $G(x) = F_x(0\ldots0)\|F_x(1\ldots1)$, where x is a 128-bit input.

2. Let G be a pseudorandom generator and define $G_0(s)$ to be the output of G truncated to n bits (where s is of length n). Prove that the function $F_k(x) = G_0(k) \bigoplus x$ is not a pseudorandom function.

3. Prove that any pseudorandom permutation is also a pseudorandom function.

4. Let $(Gen; Enc; Dec)$ be an encryption scheme defined as follows:

   (a) Gen outputs a key k for a pseudorandom permutation F.

   (b) Upon input $m \in \{0,1\}^{n/2}$ and key k, algorithm Enc chooses a random string $r \leftarrow \{0,1\}^{n/2}$ of length $n/2$ and computes $c = F_k(r|m)$. Show how to decrypt, and prove that this scheme is CPA-secure.