MATH 3540 **Name:** _____
Homework 3

Directions

1. Complete the following questions.

---

1. Consider a pseudo one-time pad encryption scheme Π constructed using some function G. Which of the following did our proof of security for the pseudo one-time pad show?

   (a) If G is a pseudorandom generator, then Π is perfectly secret.

   (b) Π is always computationally secret, for any G.

   (c) Π is always perfectly secret, for any G.

   (d) If G is a pseudorandom generator, then Π is computationally secret.

2. Define the following function G taking n-bit inputs and producing (n+1)-bit outputs: $G(x) = x|0$, where | denotes concatenation. Construct an attack that shows this G is not a pseudorandom function.

3. Let G be a pseudorandom generator where $|G(s)| = 2|s|$.

   (a) Define $G_0(s) = G(so^{|s|})$. Is G_0 necessarily a pseudorandom generator?

   (b) Define $G_0(s) = G(s_1 \dots s_{n/2})$ where $s = s_1 \dots s_n$. Is G_0 necessarily a pseudorandom generator?

4. Show the following Theorem: Let n_1 and n_2 be negligible functions. Then n_1+n_2 is negligible.