MATH 3540 **Name:** _____
Day 7

Directions

1. Complete the following questions.

---

1. Let G be a pseudorandom generator where $|G(s)| = 2|s|$. Define $G_0(s) = G(so^{|s|})$. Is G_0 necessarily a pseudorandom generator?

2. Show that the pseudo-OTP is not multiple-message indistinguishable