Answer ALL of the following questions with "yes" or "no". You MUST also explain your answer.

/0 (2pts) **Q1:** Let M = C = K = {0, 1, 2, … , 255} and consider the following cipher defined over (K, M, C):

E(k, m) = m + k (mod 256) ; D(k, c) = c − k (mod 256).

Does this cipher have perfect secrecy?

~~Yes, because t~~

No, because i can encrypt the cipher text and change in the message text (no integrity).

/4 (4pts) **Q2:** Let (E, D) be a (one-time) semantically secure cipher where the message and ciphertext space is $\{0, 1\}^n$. Which of the following encryption schemes are (one-time) semantically secure?

a. E′ (k, m) = 0 ‖ E(k, m)

Semantically secure, because i cant distinguish two plaintext messages from the cipher text.

b. E′ (k, m) = E(k, m) ‖ LSB(m)

Not semantically secure, because the LSB of the message in the cipher can determine for which message is this.

/1 (2pts) **Q3:** Let G : $\{0, 1\}^s \rightarrow \{0, 1\}^n$ be a secure PRG. Is the following PRG secure:

G′ (k) = G(k)[0, … , n − 2], (i.e., G′ (k) drops the last bit of G(k))

Yes, [0,...,n-2] ~~can~~ does it ~~make~~ sense.

/1 (2pts) **Q4:** Let F : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a secure PRF (i.e. a PRF where the key space, input space, and output space are all $\{0, 1\}^n$) and say n = 128. Is the following PRF secure:

F′ (k, x) = F(k, x) ‖ 0

No, because F'(k,x) can have more than one value of x.