Assignment 2

Submission Deadline: 2021.9.29, 12:00pm

1. Let $G: \{0,1\}^s \rightarrow \{0,1\}^n$ be a secure PRG. Which of the following is a secure PRG (could be more than one), and give your explanation.

$G'(k_1, k_2) = G(k_1)||G(k_2)$
$G'(k) = G(0)$
$G'(k) = G(k)$
$G'(k) = G(k)||0$
$G'(k) = G(k \oplus 1^s)$
$G'(k) = reserver(G(k))$, where reverse(x) reverses the string x so that the first bit of x is the last bit of reverse(x) and so on.

2. Let $G: K \rightarrow \{0,1\}^n$ be a secure PRG. Define $G'(k_1, k_2) = G(k_1) \wedge G(k_2)$ where $\wedge$ is the **bit-wise AND function**. Consider the following statistical test A on $\{0,1\}^n$. A(x) outputs LSB(x), the least significant bit of x. What is the $Adv_{PRG}[A, G']$? You may assume that LSB(G(k)) is 0 for exactly half the seeds k in K.

3. 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 scheme are semantically secure? Give your explanation for each of the options.

1) $E'\big((k, k'), m\big) = E(k, m)||E(k', m)$
2) $E'(k, m) = E(0^n, m)$
3) $E'(k, m) = E(k, m)||k$
4) $E'(k, m) = E(k, m)||LSB(m)$

4. Suppose you are told that the one time pad encryption of the message "attack at dawn" is 6c73d5240a948c86981bc294814d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "attack at dusk" under the same OTP key?