Cryptography HW 1 (deadline: October 11)

Problem 1 [15pt]. Let $G : \{0,1\}^s \to \{0,1\}^n$ be a secure PRG. Prove or disprove that the following PRGs are secure (there may be more than one correct answer). Justify your answer.

- $G_1(k) = G(k) \bigoplus 1^n$
- $G_2(k_1, k_2) = G(k_1) \parallel G(k_2)$ (here $\parallel$ denotes a concatenation)
- $G_3(k) = G(k) \parallel G(k)$
- $G_4(k) = G(k) \parallel 0$
- $G_5(k) = rev(G(k))$ where $rev(x)$ reverses the string x so that the first bit of x is the last bit of $rev(x)$, the second bit of x is the second to last bit of $rev(x)$, and so on.

Problem 2 [15pt]. 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 or not? Justify your answer.

- $E_1((k, k'), m) = E(k, m) \parallel E(k', m)$
- $E_2(k, m) = E(k, m) \parallel \mathrm{LSB}(m)$
- $E_3(k, m) = E(k, m) \parallel k$
- $E_4(k, m) = E(0^n, m)$

Problem 3 [10pt]. The OTP encryption scheme has perfect secrecy (refer the 24 slide of lecture note #2).

Problem 4 [15pt]. Let $G : K \to \{0,1\}^n$ be a secure PRG. Define $H(k_1, k_2) = G(k_1) \vee G(k_2)$ where $\vee$ is the bit-wise OR function. Consider the following statistical test $\mathcal{A}$ on $\{0,1\}^n$:

$$\mathcal{A}(x) \text{ outputs } \mathrm{LSB}(x),$$

where $\mathrm{LSB}(x)$ denotes the least significant bit of x. Calculate $Adv_{PRG}[\mathcal{A}, H]$.

Problem 5 [15pt]. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF (i.e., key, input and output spaces are all $\{0,1\}^n$) for $n = 128$. Which of the following is a secure PRF? Justify your answer.

- $F_1(k, x) = F(k, x)[0, \ldots, n-2]$ (i.e., F_1 drops the last bit of F)
- $F_2(k, x) = F(k, x) \parallel 0$
- $F_3((k_1, k_2), x) = F(k_1, x) \parallel F(k_2, x)$
- $F_4(k, x) = \begin{cases} F(k,x) & \text{if } x \neq 0^n \\ 0^n & \text{otherwise} \end{cases}$

Problem 6 [15pt]. Let $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a secure PRF. Define $G : \mathcal{K} \to \{0,1\}^{nt}$ by

$$G(k) = F(k, 1) \| F(k, 2) \| \cdots \| F(k, t).$$

Is G a secure PRG? Justify your answer.

Problem 7 [15pt]. DES-X augments DES by XORing an extra 64 bits of key (k_1) to the plaintext before applying DES with the key k, and then XORing another 64 bits of key (k_2) after the encryption:

$$\text{DES-}X(m) := k_2 \oplus \text{DES.Enc}(k, m \oplus k_1).$$

Describe a simple attack on DES-X with complexity 2^{120}.