Homework 3: more PRGs, Security Reductions, CPA, PRFs

Submission policy. Submit your answers on Blackboard by 11:59pm Friday, **Oct. 1**, 2021. Your submission should include a .PDF file with all the answers to the theoretical problems. You should try to typeset your homeworks. Latex is especially recommended. No late submissions will be accepted. Your writeup MUST include the following information:

1. Your name and whether you take the class at **487** or **587** level.
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

The homework will be graded by the class TA Anuj Pokhrel (apokhre@gmu.edu).

Exercise 1. ONLY IF in 587 level [20 points]
Recall the definition of indistinguishability for multiple encryptions in the presence of an eavesdropper (this Definition 3.19 in [KL]). In this definition there is no restriction on what messages the adversary includes in $\vec{M}_0, \vec{M}_1$ (i.e. the same message might appear in different positions within $\vec{M}_0$ (or $\vec{M}_1$) and the same message can appear in both $\vec{M}_0, \vec{M}_1$).
Now consider a modification of this definition where *all* the messages within $\vec{M}_0$ are distinct, and similarly for $\vec{M}_1$, but a message may still appear in both $\vec{M}_0$ and $\vec{M}_1$.

(a) Show that Construction 3.17 does not satisfy this new definition. (You have to show how an adversary can pick $\vec{M}_0, \vec{M}_1$ to break the definition and compute its success probability)

(b) Give a construction of a **deterministic** (stateless) encryption scheme that satisfies your definition.

Exercise 2. PRGs [30 points]
Assume that $H : \{0,1\}^n \to \{0,1\}^{2n}$ is a secure PRG, then prove that $G(s_L||s_R) = s_L||H(s_R)$ is also a secure PRG (where $s = s_L||s_R$ and $|s_L| = |s_R|$ (you can assume n is always even).
You can break down your answer as follows:

(a) (5 points) State the contrapositive you will be proving.

(b) (15 points) Design the reduction (i.e. how the two distinguishers interact with each other).

(c) (10 points) Analyze the probability of success of your reduction.

Exercise 3. Pseudorandom Functions [40 points] Let $F_k : \{0,1\}^n \mapsto \{0,1\}^n$ be a pseudorandom function.

For each of the functions below you will have to show that it is NOT a PRF,i.e., give an attack and a justification for why your attacker/distinguisher can distinguish whether it is talking to a pseudorandom function or a truly random function with probability $1/2 + p(n)$ where $p(n)$ is a non-negligible value.

a. (20 points) Show that $F_k^a(x) = F_k(0||x)||F_k(x||1)$, where $||$ denotes string concatenation, is NOT a PRF.

b. (20 points) Show that $F_k^b(x) = F_k(x) \oplus F_k(\bar{x})$ is NOT a PRF. The bar notation, , denotes inversion of the string, i.e. if $x = 01101$, then $\bar{x} = 10010$.

Exercise 4. CPA Encryption [30 points] In this question you will break CPA security of two encryption schemes (the first build with PRGs and the second build with PRFs).

(a) State the CPA security game (3 points).

Consider the following encryption scheme:

Let $G() : \{0,1\}^n \to \{0,1\}^{2n}$ be a secure PRG.

$\mathsf{Gen}(1^n)$: Output a key k of size n bits selected uniformly at random from $\{0,1\}^n$
$\mathsf{Enc}(k,m) : c = m \oplus G(k) \oplus 1^{|2n|}$ (where $1^{|n|}$ is a string of all 1's of size n)
$\mathsf{Dec}(k,c) : m = c \oplus G(k) \oplus 1^{|2n|}$
Show that the above construction is **not** CPA-secure.

(b) Describe an adversary that can break CPA security of above construction (8 points).

(b) Explicitly state the probability of success of this adversary (5 points).

Now consider another construction:Let F be a fixed-length PRF.

$\mathsf{Gen}(1^n) : k \leftarrow \{0,1\}^n$
$\mathsf{Enc}(k,m) : F_k(0^n) \oplus m$
$\mathsf{Dec}(k,c) : F_k(0^n) \oplus c$
Show that the above construction is **not** CPA-secure.

(b) Describe an adversary that can break CPA security of the above construction (8 points).

(b) Explicitly state the probability of success of this adversary (6 points).