Homework 3

1 Problem 1 (15 points)

Let PRG be a pseudorandom generator. Consider the following attempt at building a stateless many-use encryption scheme. $\mathsf{Enc}(k, m)$ chooses a random string IV of length λ (here, λ is the length of the key), and then runs $x \leftarrow \mathsf{PRG}(IV, k)$ (that is, run PRG on the string obtained by concatenating IV and k). Finally, it computes $c \leftarrow x \oplus m$. The ciphertext is the pair (IV, c). $\mathsf{Dec}(k,\ (IV, c)\ )$ uses IV and k to compute x, and XOR's x and c to recover m.

Devise an example of a PRG PRG such that the above encryption scheme using PRG is insecure *even for a single message*. That is, PRG should satisfy the definition of a secure PRG, but Enc should not satisfy one-time computational security.

You may assume as a building block a secure pseudorandom generator PRG', which you can use to build your PRG. Your construction must work (that is, yield an insecure encryption scheme) for any PRG', as long as PRG' is a secure PRG; do not assume any particular structure on PRG'. Remember to prove the security of PRG assuming the security of PRG' using a reduction.

2 Problem 2 (25 points)

Let PRF be a pseudorandom function with domain $\{0,1\}^m$ and range $\{0,1\}^n$. Prove that the following are each also pseudorandom functions:

- PRF_a has domain $\{0,1\}^{m-1}$ and range $\{0,1\}^{2n}$. $\mathsf{PRF}_a(k, x) = \mathsf{PRF}(k, x||0)||\mathsf{PRF}(k, x||1)$.
- Assume $n = 2^k$. PRF_b has domain $\{0,1\}^{m+k}$ and range $\{0,1\}$. Given an input $x \in \{0,1\}^{m+k}$, partition x as $x' \in \{0,1\}^m$ and $i \in \{0,1\}^k$. $\mathsf{PRF}_b(k, x'||i) = \mathsf{PRF}(k, x')_i$. That is, output the ith bit of $\mathsf{PRF}(k, x')$.
- Let $h : \{0,1\}^\ell \to \{0,1\}^m$ be any injective function (that is, a function where there do not exist any pairs of inputs $x \neq y$ such that $h(x) = h(y)$). PRF_c has domain $\{0,1\}^\ell$ and range $\{0,1\}^n$, and is defined as $\mathsf{PRF}_c(k, x) = \mathsf{PRF}(k, h(x))$.
- Let PRG be a secure PRG. Assume $n = \lambda$. Define $\mathsf{PRF}_d(k, x) = \mathsf{PRG}(\mathsf{PRF}(k, x))$.

3 Problem 3 (10 points)

Let PRF be a pseudorandom function with domain $\{0,1\}^m$ and range $\{0,1\}$. Assume $m > \log \lambda$. Use PRF to construct a secure PRG, and prove its security assuming only the security of PRF.

4 Problem 4 (50 points)

Consider the following notions of security for encryption schemes.

(i) **Left-or-Right (LoR) Indisitnguishability**. This is the notion of security we saw in class

(ii) **Real-or-Random Plaintext (RoRP) Indistinguishability**. This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If it's input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challenger's input bit is $b = 1$, then the challenger chooses a new random message m' and encrypts m' to get a ciphertext c, which it then returns to the adversary. Security is defined in the usual way: for any efficient adversary A, there is a negligible function $\epsilon(\lambda)$ such that the adversary has at most $\epsilon(\lambda)$ advantage in distinguishing $b = 0$ from $b = 1$.

(iii) **Real-or-Random Ciphertext (RoRC) Indistinguishability**. This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If it's input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challenger's input bit is $b = 1$, then the challenger chooses a random string c in the ciphertext space $\mathcal{C}$, which it then returns to the adversary. Security is defined in the usual way: for any efficient adversary A, there is a negligible function $\epsilon(\lambda)$ such that the adversary has at most $\epsilon(\lambda)$ advantage in distinguishing $b = 0$ from $b = 1$.

(iv) **Real-or-Zero (RoZ) Indistinguishability**. This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. The challenger responds to the queries as follows. If it's input bit is $b = 0$, then the challenger encrypts m to get a ciphertext c, which it returns to the adversary. If the challenger's input bit is $b = 1$, then the challenger encrypts $m' = 0$ to get a ciphertext c, which it then returns to the adversary. Security is defined in the usual way:

for any efficient adversary A, there is a negligible function $\epsilon(\lambda)$ such that the adversary has at most $\epsilon(\lambda)$ advantage in distinguishing $b = 0$ from $b = 1$.

Some of these notions are equivalent (in the sense that if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies one notion, then it must also satisfy the other), and some are stronger than others (in the sense that if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies notion (a), it must satisfy notion (b), but there are examples of schemes that satisfy (b) but not (a)). Your goal is to figure out the relationships between each of these security notions.

Your solution will contain several proofs of statements of the form: "if $(\mathsf{Enc}, \mathsf{Dec})$ satisfies notion (a), then it also satisfies notion (b)" (this can succinctly be stated as "notion (a) implies notion (b)").

Note that you do not necessarily need to prove all implications: if notion (a) implies notion (b) and notion (b) implies notion (c), then you can conclude without proof that notion (a) also implies notion (c).

Your solution will also contain some proofs of statements of the form: "There exist $(\mathsf{Enc}, \mathsf{Dec})$ satisfying notion (a) but that does not satisfy notion (b)" (this can be succinctly stated as "notion (a) does not imply notion (b)). For these kind of statements, you may assume as a starting point a secure PRG, a secure PRF, or an encryption scheme satisfying any of the notions above (LoR, RoRP, RoRC,RoZ), which you then use to build your $(\mathsf{Enc}, \mathsf{Dec})$ counter example.

Again, note that you do not necessarily need to prove all implications. For example, if (a) does not imply (b), but (c) *does* imply (b), then you can conclude without proof that (a) does not imply (c).

There are a total of 12 statements to decide on (for every pair of notions (a) and (b), you must decide whether or not (a) implies (b) and whether or not (b) implies (a)). As a hint, it is possible to select 5 statements, prove those, and then derive the remaining 7 from these 5. You will not be penalized or rewarded based on the number of statements you prove; if you prove all 12 directly, that is fine (though it will be more work on your part).

5 Bonus: Problem 5 (10 points)

Consider the following additional security notion:

(v) **Real-or-Complement (RoC) Indistinguishability**. This security notion is defined by the following experiment. The adversary makes polynomially-many queries to the challenger on messages m in the message space. Assume the message space is $\{0,1\}^n$ for some n. The challenger responds to the queries as follows. If it's input bit is $b = 0$, then the challenger encrypts m to get a

ciphertext c, which it returns to the adversary. If the challenger's input bit is $b = 1$, then the challenger encrypts $m' = m \oplus 1^n$ — the bitwise complement of m — to get a ciphertext c, which it then returns to the adversary. Security is defined in the usual way: for any efficient adversary A, there is a negligible function $\epsilon(\lambda)$ such that the adversary has at most $\epsilon(\lambda)$ advantage in distinguishing $b = 0$ from $b = 1$.

Add this notion to Problem 4, and decide how this notion relates to the other four notions as you did before. There are 8 more statements to decide on (two statements each for comparing RoC to the notions from Problem 4. As before, some of the statements can be derived from others).