CSE 546
Modern Cryptography

Homework 1

September 1, 2022

Important: The deadline for Homework 1 is **1:00 pm on 9/8/2022**. Since we will discuss the solutions during the lecture, late submissions *will not be accepted.*

Instructions:

- This homework assignment is worth 115 points. You can score a maximum of 100 points (i.e. there is a 'bonus' of 15 points). You can attempt questions accordingly.
- While discussing problems with your classmates is allowed, your answers *must be in your own words.* Any exceptions will be punished, extending to reporting plagiarism according to departmental regulations. We know the online resources you would find for these problems, so use them at your own risk :)
- Be clear, succinct, and precise, but most importantly, be *rigorous.* Points not made are points lost.

Problem 1: Perfect Security

Consider a modification of one-time pad (Vernam's cipher), where the message space $\mathcal{M}$, ciphertext space $\mathcal{C}$ are equal to $\{0,1\}^{\ell}$. While the key space K is equal to $\{0,1\}^{2\ell}$ (the set of all binary strings of length 2ℓ).
Gen chooses a uniform key k from the key space K. Key k can be abstracted as divided into two halves k_1 being the first ℓ bits and k_2 being the second ℓ bits.
$\mathsf{Enc}_k(m) = m \oplus k_1 \oplus k_2$
$\mathsf{Dec}_k(c) = c \oplus k_1 \oplus k_2$

(i) **(5 pts)** State whether the given modified scheme is perfectly secret. Justify your answer.

(ii) **(5 pts)** Note that in the scheme above, there would be a scenario where randomly selected key k has equal halves. Do you think perfect secrecy claim would be violated due to this scenario, if yes, present formal proof. If not, reconcile the scenario with original one-time pad scheme's scenarios.

(iii) **(5 pts)** In this part, we modify *Gen* to construct key k in this way: randomly sample a key k' from $\{0,1\}^{\ell}$. Given a fixed string α (of the same size as k'), $k = k'||(k' \oplus \alpha)$ ($||$ denotes concatenation). If Enc, Dec are kept the same, would this scheme be perfectly secret? Justify your answer.

Problem 2: Negligible functions

Recall that negligible functions serve as a crucial ingredient in proofs of security for various primitives. This is primarily due to the fact that these functions capture the notion of 'allowable success' for adversaries in a robust and intuitive manner. We will examine this further in the following questions. Familiarity with section 3.1 of the course text will help.

(i) **(5 pts)** Prove or refute: let $p()$ be a polynomial and $\nu()$ be a negligible function. Consider a function $g(n)$ that equals $\frac{1}{p()}$ when n is a multiple of 100, and equals $\nu(n)$ otherwise. Then g is negligible.

(ii) **(5 pts)** Prove or refute: let $\nu()$ be a negligible function and α be an arbitrary constant. Consider a function $f(n) = 2^{\alpha}\nu(n)$. Then f is negligible.

Problem 3: PRGs

Let G be a pseudorandom generator with expansion factor $l(n) = 3n$. In each of the following cases, say whether G' is necessarily a pseudorandom generator (infer expansion factor of G' from the return values). If yes, give a proof; if not, show a counterexample.

(i) **(7 pts)** $G'(s)$:

```
$x := G(s) \quad y := G(0^{\alpha})$
return $x||y$
```

(ii) **(7 pts)** $G'(s)$:

```
$x := G(x) \quad y := G(0^{\alpha})$
return $x \oplus y$
```

(iii) **(7 pts)** $G'(s)$:

```
$x := G(s) \quad y := G(s)$
return $x||y$
```

(iv) **(7 pts)** When we write $a||b||c := G(s)$, each of a, b, c have length n -

```
$G'(s)$ :
$x||y||z := G(s)$
return $x||y$.
```

Problem 4: More PRGs

(25 Points) Again suppose that you are given a PRG $G : \{0,1\}^n \longrightarrow \{0,1\}^{2n}$. Define a new function $G^* : \{0,1\}^n \longrightarrow \{0,1\}^{2n}$ as follows: given input an n-length bit string s, G^* works as follows:

- Computes $t = G(s)$.

- Picks an arbitrary index i from $[n] = \{1, \ldots, n\}$, and sets t' to be the substring of t of length n starting at index i.
- Computes $G(t')$ and outputs this value.

Prove or disprove that G^* as defined is a PRG.

Problem 5: Passive Encryption

This question will test your understanding of the definitions used to define indistinguishable encryptions in the presence of an eavesdropper.

(i) **(17 Points)** In the lecture, we saw two definitions for **indistinguishable encryptions in the presence of an eavesdropper** (Definition 3.8 and 3.9 in Chapter 3.2.1, Page 55 in the course text). Prove that these two definitions are equivalent.

(ii) **(20 Points)** Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary length messages and the adversary is not restricted to output equal length messages in experiment $PrivK^{eav}_{\mathcal{A},\Pi}$