Intro to Cryptography
Portland State U, Winter 2017

Homework 2

JANUARY 24

Instructor: Fang Song

Due by the **start of class on TUESDAY, FEBRUARY 7**. Start early!

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea.

You may collaborate with others on this problem set . However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (Perfect Secrecy)
   (a) (8 points) (3.b from HW1) [KL: Exercise 2.5] Prove Lemma 2.6. (Hint: you need to prove both directions.)
   (b) (Bonus 10 points) (3.c from HW1) Suppose E is an encryption with key of length n and messages of length $\geq n + 10$. Show that there exist two messages m_0, m_1 and a strategy for an eavesdropper Eve so that given a ciphertext $c = E_k(m_b)$ for random k and random $b \in \{0, 1\}$, Eve can output m_b with probability at least 0.99.
   (c) (4 points) [KL: Exercise 2.7] When using one-time pad with key $k = -^{\ell}$, we have $E_k(m) = k \oplus m = m$, and the message is sent in the clear! It is therefore suggested to modify one-time-pad by only using a random non-zero key k. Is this modified scheme still perfectly secret? Justify your answer. (Hint: reading [KL: Section 2.4] would be helpful.)

2. (Asymptotic) (Problem 4 from HW1) Recall the following definitions
   - A non-negative function $f \colon \mathbb{N} \to \mathbb{R}$ is *polynomially bounded*, written $f(n) = \mathrm{poly}(n)$, if $f(n) = O(n^c)$ for some constant $c \geq 0$.
   - A non-negative function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is *negligible*, written $\varepsilon(n) = \mathrm{negl}(n)$, if it decreases faster than the inverse of any polynomial. Formally: $\lim_{n\to\infty} \varepsilon(n) \cdot n^c = 0$ for any constant $c \geq 0$. (Otherwise, we say that $\varepsilon(n)$ is *non-negligible*.)

   (a) (3 points) Is $\varepsilon(n) = 2^{-100 \log n}$ negligible or not? Prove your answer. (Why doesn't the base of the logarithm matter?)
   (b) (3 points) Suppose that $\varepsilon(n) = \mathrm{negl}(n)$ and $f(n) = \mathrm{poly}(n)$. Is it always the case that $f(n) \cdot \varepsilon(n) = \mathrm{negl}(n)$? If so, prove it; otherwise, give concrete functions $\varepsilon(n), f(n)$ that serve as a counterexample.

3. (6 points) (Computational secrecy) [KL: Exercise 3.2] 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 $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$. (This result implies that it is *impossible* to support encrypting arbitrary-length messages while hiding all information about the plaintext length. Most commonly used encryption schemes do actually reveal the plaintext length.)

4. (12 points) (Pseudorandom generators) [KL: Exercise 3.6] Let G be a psuedorandom generator with expansion factor $\ell(n) > 2n$. Decide if each of the following construtions G' is a psuedorandom generator. If yes, give a proof; if not, show a counterexample.

i) $G'(s) := G(s_1, \ldots, s_{\lfloor n/2 \rfloor})$, where $s = s_1, \ldots, s_n$.

ii) $G'(s) := G(0^{|s|} \| s)$.

iii) $G'(s) := G(s) \| G(s+1)$.

5. (Pseudorandom functions)

   (a) (6 points) [KL: Excersice 3.9] Prove *unconditionally* the existence of a pseudorandom function $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ with $\ell_{key}(n) = n$ and $\ell_{in}(n) = O(\log n)$.

   (b) (8 points) [KL: Excersice 3.10] Let F be a length-preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, decide whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

      i) $F'_k(x) := F_k(0\|x) \| F_k(1\|x)$.

      ii) $F'_k(x) := F_k(0\|x) \| F_k(x\|1)$.