Winter 2018 CS 485/585 Introduction to Cryptography

Homework 1

Portland State University — *Jan. 09, 2018*
Lecturer: Fang Song — *Due: Jan. 18, 2018*

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. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them. The .tex source is provided on course webpage as a template if you want to typeset your solutions in Latex.

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. (Probability)
   (a) (Exercise. Do not turn in.) Let $E[\cdot]$ be the expectation. Describe two random variables X_1 and Y_1 such that $E[X_1 \cdot Y_1] = E[X_1] \cdot E[Y_1]$. Describe another two random variables X_2 and Y_2 such that $E[X_2 \cdot Y_2] \neq E[X_2] \cdot E[Y_2]$.
   (b) (5 points) Suppose there is a new test for a medical condition, and it has the following error rates:
   - False positive: if you do not have the condition, there is a 5% chance that the test comes positive.
   - False negative: if you have the condition, there is 10% chance that the test comes negative.

   Assuming incidence of this condition occurs in 1% of the population. How likely that a person tested positive indeed has this condition?
   (c) (5 points) Consider a biased coin that appears HEADS with probability p. We flip it multiple times independently. What is the expected number of trials until you see HEADS for the first time?
   (d) (Bonus 5pts) Suppose that a certain brand of cereal includes a free coupon in each box. There are n different types of coupons. How many boxes do you expect to buy before finally getting a coupon of each type? (Hint: the harmonic number $H(n) := \sum_{i=1}^{n} \frac{1}{i} = \Theta(\log n)$.)

2. (Asymptotic notations) Recall the following definitions
   - A non-negative function $f\colon \mathbb{N} \to \mathbb{R}$ is *polynomially bounded*, written $f(n) = \text{poly}(n)$, 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 $\varepsilon(n) = \text{negl}(n)$, 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 $\varepsilon(n) = 2^{-10^6 \log^3 n}$ negligible or not? Prove your answer. (Why doesn't the base of the logarithm matter?)

(b) (3 points) Suppose that $\varepsilon(n) = \text{negl}(n)$ and $f(n) = \text{poly}(n)$. Is it always the case that $f(n) \cdot \varepsilon(n) = \text{negl}(n)$? If so, prove it; otherwise, give concrete functions $\varepsilon(n), f(n)$ that serve as a counterexample.

3. (Perfect Secrecy)

(a) (8 points) [KL: Exercise 2.5.] Prove Lemma 2.6. (Hint: you need to prove both directions.)

(b) (4 points) [KL: Exercise 2.7] When using one-time pad with key $k = 0^\ell$, 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.

4. (Computational secrecy)

(a) (5 points) [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 $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

(b) (5 points) [**G**] [KL: Exercise 3.3]

5. (Pseudorandom generators)

(a) (8 points) [KL: Exercise 3.5]

(b) (4 points) Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. Define $G'(s) := G(s) \| G(s+1)$. Is G' necessarily a pseudorandom generator? If so, give a proof; otherwise, show a counterexample.