**Intro to Cryptography** | **Portland State U, Winter 2017**

# Homework 1

JANUARY 10

**Instructor: Fang Song**

Due by the **start of class on TUESDAY, JANUARY 24**. 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. (5 points) (**Attention: this problem is due Tuesday, January 17, 11:59pm PST.**) Send an email to me (`fsong@pdx.edu`) with subject "`CS 485/585 student`" describing: 1) a few words about yourself and background (department, program, etc.), 2) what you hope to get out of this course, and 3) your confidence level (0-5) with: mathematical proofs, probability theory, algorithm analysis, Turing machines, complexity classes such as $\mathsf{P}$, $\mathsf{NP}$, $\mathsf{NP}$-completeness.

2. (20 points) (Probability). Let $X, Y$ be random variables over some sample space $\Omega$. $\mathrm{E}[\cdot]$ denotes expectation.

   (a) (3 points) Give an example of two random variables $X, Y$ such that $\mathrm{E}[XY] = \mathrm{E}[X]\,\mathrm{E}[Y]$.

   (b) (3 points) Give an example of two random variables $X, Y$ such that $\mathrm{E}[XY] \neq \mathrm{E}[X]\,\mathrm{E}[Y]$.

   (c) (5 points) Define the variance $Var[X] = \mathrm{E}[(X - \mathrm{E}[X])^2]$. Prove that $Var[X]$ is always non-negative.

   (d) (5 points) Let $X$ be the number of `HEADS` after $n$ fair coin tosses. Calculate $\mathrm{E}[X]$. (Hint: use linearity of expectation)

   (e) (4 points) Let $X$ be as in part (d). Show that $\Pr[X \geq 0.6n] \leq 0.85$.

3. (Perfect Secrecy)

   (a) (5 points) Consider the (mono-alphabetic) substitution cipher where the key is a uniformly random permutation of the alphabet. If we encrypt *just one message* that is *shorter than the alphabet size*. Is this perfectly secret? You must justify your answer with a convincing argument.

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

   (c) (Bonus 10 points) 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 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.

4. (Asymptotic) 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.

5. (6 points) (Taste of research frontier) Pick one talk you attended (or video you watched), describe 1) its main topic, 2) the application/connection to cryptography, and 3) one open question in its research area. For more information, read at `http://www.fangsong.info/teaching/w17_4585_icrypto/#mu`.