Theoretical Foundations of Cryptography **Instructor: Chris Peikert**
Georgia Tech, Spring 2011 **Student: YOUR NAME HERE**

Homework 1

This homework is due by the **start of class on January 27** via the course page on T-Square. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness*, *clarity*, and *conciseness*. 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 and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators/sources*** for each problem.

1. (5 points) *(Due by mid-day on Wed, Jan 19.)* Send email to Chris (`cpeikert@cc.gatech.edu`) with subject `8803TFC student` containing (1) a few sentences about yourself and your background (including your department and graduate program), (2) what you hope to get out of this course, and (3) your comfort level with the following: mathematical proofs, elementary probability theory, big-O notation and analysis of algorithms, Turing machines, and P, BPP, NP, and NP-completeness. Please also mention any courses you've taken covering these topics.

2. *(Perfect secrecy.)* Prove or disprove (giving the simplest counterexample you can find) the following statements about perfect secrecy for shared-key encryption. You may use any of the facts from class.

   (a) (2½ points) There is a perfectly secret encryption scheme for which the ciphertext always reveals 99% of the bits of the key k to the adversary.

   (b) (2½ points) In a perfectly secret encryption scheme, the ciphertext is uniformly random. That is, for every $m \in \mathcal{M}$, the probability $\Pr_{k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m) = \bar{c}]$ is the same for every ciphertext $\bar{c} \in \mathcal{C}$.

   (c) (5 points) Perfect secrecy is equivalent to the following definition, which says that the adversary cannot determine which of two messages was encrypted any better than by random guessing. Formally, for any $m_0, m_1 \in \mathcal{M}$, and any function $\mathcal{A} : \mathcal{C} \to \{0,1\}$,

   $$\Pr_{k \leftarrow \mathsf{Gen},\, b \leftarrow \{0,1\}}[\mathcal{A}(\mathsf{Enc}_k(m_b)) = b] = \frac{1}{2}.$$

   (d) (5 points) Perfect secrecy is equivalent to the following definition, which says that the ciphertext and message are independent (as random variables). Formally, for any probability distribution $\mathcal{D}$ over the message space $\mathcal{M}$ and any $\bar{m} \in \mathcal{M}$ and $\bar{c} \in \mathcal{C}$,

   $$\Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}[m = \bar{m} \wedge \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow \mathcal{D}}[m = \bar{m}] \cdot \Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m) = \bar{c}].$$

3. *(Working with negligible functions.)* Recall that a non-negative function $\nu : \mathbb{N} \to \mathbb{R}$ is *negligible* if it decreases faster than the inverse of any polynomial (otherwise, we say that ν is *non-negligible*). More precisely, $\nu(n) = o(n^{-c})$ for every fixed constant $c > 0$, or equivalently, $\lim_{n\to\infty} \nu(n) \cdot n^c = 0$.

   State whether each of the following functions is negligible or non-negligible, and give a brief justification. In the following, $\mathrm{negl}(n)$ denotes some arbitrary negligible function, and $\mathrm{poly}(n)$ denotes some arbitrary polynomial in n.

   (a) (1 point) $\nu(n) = 1/2^{100 \log n}$.

   (b) (1 point) $\nu(n) = n^{-\log\log\log n}$. (Compare with the previous item for "reasonable" values of n.)

(c) (1 point) $\nu(n) = \mathrm{poly}(n) \cdot \mathrm{negl}(n)$. (State whether ν is *always* negligible, or not necessarily.)

(d) (1 point) $\nu(n) = (\mathrm{negl}(n))^{1/\mathrm{poly}(n)}$. (Same instructions as previous item.)

(e) (1 point)

$$\nu(n) = \begin{cases} 2^{-n} & \text{if } n \text{ is composite} \\ 100^{-100} & \text{if } n \text{ is prime.} \end{cases}$$

4. *(Working with one-way functions.)*

(a) (5 points) Suppose that $f : \{0,1\}^* \to \{0,1\}^*$ is such that $|f(x)| \leq c \log|x|$ for every $x \in \{0,1\}^*$, where $c > 0$ is some fixed constant. (Here $|\cdot|$ denotes the length of a string.)

Prove that f is *not* a one-way function. (You may use a *non-uniform* inverter in your solution; for one bonus point, use a uniform one.)

(b) (5 points) Finish the proof of the hardness amplification theorem from the lecture, i.e., define and analyze the algorithm $\mathcal{A}$ that uses $\mathcal{A}'$. You may use any of the ideas and facts from the lecture notes.

(c) (5 points) Prove that there exists a collection $\{f_i\}$ of one-way functions if and only if there exists a one-way function f. (*Hint*: incorporate the collection's generation algorithm Gen, and its randomness, into the definition of f.)