Introduction to Cryptography
Courant, Fall 2015

Homework 1

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **7am of Sep 21**. Send by email to both "regev" (under the cs.nyu.edu domain) and "mgeorgiou@nyu.edu" with subject line "CSCI-GA 3210 Homework 1" and name the attachment "YOUR NAME HERE HW1.tex/pdf". No need for a printed copy. 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 are expected to read all the hints either before or after submission, but before the next class.

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

1. (5 points) *(Shannon)* Prove that in any perfectly secret shared-key encryption scheme, $|\mathcal{K}| \geq |\mathcal{M}|$.

   Solution:

2. *(Perfect secrecy.[1])* 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) (1 point) There is a perfectly secret encryption scheme for which the ciphertext always reveals 99% of the bits of the key k to the adversary.

   Solution:

   (b) (2 points) There is an encryption scheme that is not perfectly secure, yet the adversary cannot guess the key with probability greater than $1/|\mathcal{K}|$.

   Solution:

   (c) (2 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 $\bar{c} \in \mathcal{C}$.

   Solution:

   (d) (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 $\mathcal{A} : \mathcal{C} \to \{0, 1\}$,

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

---

[1] Based on a question from Peikert's class

Solution:

(e) (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 $\bar{c} \in \mathcal{C}$,

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

Solution:

3. *(Encryption schemes with a computationally bounded adversary.)*

Consider the scenario of an encryption scheme in which Alice wants to send a message to Bob in such a way that Eve, who monitors the transmission, cannot read the message.

(a) (1 point) Explain in one sentence why Bob needs to have a secret from Eve.

Solution:

(b) (1 point) Explain in one or two sentences why Alice needs to have a secret from Eve.

Solution:

(c) (2 points) Now assume that Eve is computationally bounded (i.e., is restricted to run in polynomial time in the length of the message). Does Bob still need to have a secret from Eve? Does Alice? (your feeling for the latter is enough)

Solution:

I'm done solving and want to know more! (ID 18764)

4. (2 points) *(Defining one-way functions.*♣*)* Next class we will define the notion of a *one-way function*. Informally, this is a function $f : \{0,1\}^* \to \{0,1\}^*$ that is (1) easy to compute, and (2) hard to invert.

(a) Suggest a way (or ways) to formally define it. After thinking about this question for at least 10 minutes and before writing your solution, click here for some food for thought (ID 19166)

Solution:

Next, for each of the following functions, say if you think it's one way according to your definition.

(b) The function that given an n-bit string outputs the same string with its first half zeroed out.

Solution:

♣Questions marked with a club are more open-ended and meant to encourage you to think in preparation for next class. You are not expected to answer correctly. Instead, you are expected to spend time thinking about it.

(c) The function f on domain $\{1, \ldots, N\} \times \{1, \ldots, N\}$ that maps a pair (x, y) to their product xy.

Solution:

(d) Choose elements $a_1, \ldots, a_n$ uniformly from $\mathbb{Z}_N$ for $N = 2^n$ and define $f : \{0,1\}^n \to \mathbb{Z}_N$ by $f(b_1, \ldots, b_n) = \sum_{i=1}^n b_i a_i$.

Solution:

(e) Same as previous part, except $a_1, \ldots, a_n$ are chosen uniformly from $\mathbb{Z}_2^n$.

Solution: