Homework 1

Homework is due by **11pm of Sep 16**. Send by email to both "regev" (under the cs.nyu.edu domain) and "des480" (under the nyu.edu domain) with subject line "CSCI-GA 3210 Homework 1" and name the attachment "YOUR NAME HERE HW1.tex/pdf". There is no need to print it. Start early!

1. *(The group $\mathbb{Z}_p^*$)* Let p be an odd prime. We use $\mathbb{Z}_p^*$ to denote the multiplicative group of integers modulo p. (In mathematics the common notation is $(\mathbb{Z}/p\mathbb{Z})^*$.)
   (a) (1 point) Find an efficient algorithm that given $a \in \mathbb{Z}_p^*$ and an integer $b \geq 0$ computes $a^b \in \mathbb{Z}_p^*$. Can we simply compute a^b as integers and then reduce the result modulo p? (if not, say exactly why)
   (b) (2 points) Find an efficient algorithm to check if a given $a \in \mathbb{Z}_p^*$ is a quadratic residue.
   (c) (2 points) What fraction of the elements of $\mathbb{Z}_p^*$ are generators? How does it behave asymptotically? (You can use Wikipedia for the latter; there is no need for very precise asymptotics, just the order of magnitude)
   (d) (2 points) Describe an efficient algorithm to check if a given $g \in \mathbb{Z}_p^*$ is a generator. Assume that the algorithm is also given a factorization of $p - 1$. (It is not known how to perform this task efficiently without this factorization.)
   (e) (2 points) There is a known efficient algorithm that given a number n (in unary) outputs a uniform n-bit prime p, together with a generator g of $\mathbb{Z}_p^*$. How can that be in light of what we said earlier about the necessity of the factorization of $p - 1$? Explain the apparent paradox and suggest a solution.

2. (5 points) *(Shannon)* Prove that in any perfectly secret shared-key encryption scheme, $|\mathcal{K}| \geq |\mathcal{M}|$.

3. *(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.
   (b) (2 points) There is an encryption scheme that is not perfectly secure, yet the adversary cannot guess the key with probability greater than $1/|\mathcal{K}|$.
   (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 $\bar{c} \in \mathcal{C}$.
   (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 $\mathcal{A} : \mathcal{C} \to \{0, 1\}$,
   $$\Pr_{k \leftarrow \mathsf{Gen},\, b \leftarrow \{0,1\}}[\mathcal{A}(\mathsf{Enc}_k(m_b)) = b] = \frac{1}{2}.$$
   Hint: recall Q3c from HW0
   (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 $\bar{c} \in \mathcal{C}$,
   $$\Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}[m = \bar{m} \wedge \mathsf{Enc}_k(m) = \bar{c}] = \Pr_{m \leftarrow \mathcal{D}}[m = \bar{m}] \cdot \Pr_{m \leftarrow \mathcal{D},\, k \leftarrow \mathsf{Gen}}[\mathsf{Enc}_k(m) = \bar{c}].$$

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

4. *(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.

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

   (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)

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

5. (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)

   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.

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

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

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

♣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. Unlike normal questions (which are to be solved alone), club questions *must* be solved in groups of at least 2 students and at most 4. You must write your Latex solution alone, though. Please name the other members of group in your Latex solution. Also, one member of each group should post their solution to Piazza preferably by Thursday, but not later than 24 hours before the deadline. After a group posts to Piazza, its members should read the posts of other groups and comment. (Remember, your activity in Piazza is taken into account in the final grade.)