Homework 3

Homework is due by **noon of Sep 30**. Send by email to both "regev" and "tess" under the cs.nyu.edu domain with subject line "CSCI-GA 3210 Homework 3" and name the attachment "YOUR NAME HERE HW3.tex/pdf". Please also bring a printed copy to class. 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. (2 points) *(Expanding a PRG.*♣*)* Suggest a construction that we can use to show that the existence of a PRG with output length $\ell(n) = n + 1$ implies the existence of a PRG with any $\mathrm{poly}(n)$ output length. If you feel adventurous, try to suggest a way to prove its correctness.

2. (2 points) *(Constructing a PRG.*♣*)* Try to suggest ways to build a PRG from a OWF. For instance, say we take a one-way function $f : \{0,1\}^n \to \{0,1\}^n$. Explain why $g : \{0,1\}^n \to \{0,1\}^{2n}$ defined by $g(x) = (f(x), x)$ is not a PRG. How about $g(x) = (f(x), x_1)$? Explain how taking f to be a one-way *permutation* helps a bit, but still does not give us a PRG. Suggest a way one can try to fix the problem.

3. *(The group $\mathbb{Z}_p^*$)* Let p be an odd prime.
   (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?
   (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 might want to use Wikipedia for the latter)
   (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.

4. (2 points) Prove that there is no "statistical PRG", i.e., a (deterministic) function $g : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ for some $\ell(n) > n$ such that $g(U_n)$ is within negligible statistical distance of $U_{\ell(n)}$.

5. (5 points) [2] Prove that there exists a collection $\{f_s\}$ 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.)

♣ Another "food-for-thought" question; you are not required to solve it fully, but you are required to demonstrate that you thought about it seriously.

[2] A question from Peikert's class