Introduction to Cryptography
Courant, Fall 2013

Homework 4

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **noon of Oct 7**. Send by email to both "regev" and "tess" under the cs.nyu.edu domain with subject line "CSCI-GA 3210 Homework 4" and name the attachment "YOUR NAME HERE HW4.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. (3 points) *(Rabin's permutation)* Assume $p, q \equiv 3 \pmod 4$. Does Rabin's function remain one way when its domain is restricted to $\mathbb{QR}_N^*$ (and so becomes a one way *permutation*)?

2. *(PRGs.)*[1] Prove or disprove (giving the simplest counterexample you can find) the following statements. In constructing a counterexample, you may assume the existence of another OWF / PRG.
   (a) (4 points) Let G be a PRG with output length $\ell(n) > n$. The function $G'(s) = G(s) \oplus (s | 0^{\ell(|s|)-|s|})$ is a PRG, where $|$ denotes concatenation. I need a hint! (ID 99102)
   (b) (5 points) A PRG G with output length $\ell(n) = 2n$ is itself a one-way function. I need a hint! (ID 15489)
   (c) (4 points) (extra credit) A PRG G with output length $\ell(n) = n + 1$ is itself a one-way function. I need a hint for 1 points! (ID 19634)

3. (a) (2 points) *(Computing square roots efficiently modulo prime)* Let $p > 2$ be a prime. Assume we are given a quadratic residue $x \in \mathbb{Z}_p^*$ and we wish to compute its (two) square roots. Show that when $p \equiv 3 \bmod 4$, this can be done efficiently by computing $\pm x^{(p+1)/4}$, a formula due to Lagrange. (The case $p \equiv 1 \bmod 4$ can also be done efficiently but is more involved; feel free to look it up and summarize it here!)
   (b) (4 points) *(LSB is not hard.*[1]*)* Show how given a prime $p > 2$, a generator g of $\mathbb{Z}_p^*$, and $g^x \bmod p$ for an unknown $x \in \{0, \ldots, p-2\}$, we can efficiently decide if x is odd. (This shows that "least significant bit" [x is odd] is *not* a hard-core predicate for the modular exponentiation function $f_{p,g}(x) = g^x \bmod p$.)
   (c) (2 points) Here is a sketch of an attempt to efficiently compute discrete logs (a problem believed to be hard). Complete the missing details and identify the bug.
   We are given $y = g^x \bmod p$ for an unknown $x \in \{0, \ldots, p-2\}$. Write $x = \sum_{j=0}^{\lceil \log p \rceil} 2^j b_j$ in its binary expansion. Efficiently find b_0 as above. Let $y_1 = y/g^{b_0}$ and notice that it is a quadratic residue. Compute the square root of y_1, and continue recursively to recover all the bits of x.

4. (2 points) ♣ *(Using hard core predicates to construct PRGs)* We say that a function $h : \{0,1\}^* \to \{0,1\}$ is *hard-core* for a function f if for all non-uniform PPT algorithms $\mathcal{A}$,
$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(f(x)) = h(x)] \leq \frac{1}{2} + \mathrm{negl}(n) \ .$$
   Assume we're able to show that a certain h is hard-core for a one-way *permutation* f. Suggest a way to construct a PRG from f and h, and try to think what the analysis would entail. (We'll do the analysis in class and in the next homework.)

[1] A question from Peikert's class