Homework 6

Homework is due by **11pm of Oct 28**. 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 6" and name the attachment "YOUR NAME HERE HW6.tex/pdf". There is no need to print it. Start early!

1. (3 points) (Extra credit) Complete the proof from class, showing that "$x \geq (p-1)/2$" is a hard-core predicate for modular exponentiation.

2. *(Pseudorandom functions (PRFs))*[1] Recall that a family $\{f_s : \{0,1\}^{\ell_1(n)} \to \{0,1\}^{\ell_2(n)}\}_s$ is a *PRF family* if it is (1) efficiently computable, i.e., there exists a polynomial time F such that $F(s,x) = f_s(x)$, and (2) pseudorandom (under oracle indistinguishability), i.e., for all PPT D,

$$Adv_{\{f_s\},\{U\}}(D) := \left| \Pr_{f \leftarrow \{f_s\}}[D^f = 1] - \Pr_{f \leftarrow U}[D^f = 1] \right| = \mathrm{negl}(n) \; .$$

Let $\{f_s : \{0,1\}^n \to \{0,1\}^n\}_{s \in \{0,1\}^n}$ be a PRF family. For each of the following, say (and prove) whether it is necessarily a PRF family or not.

   (a) (1 point) $g_s(x) = f_s(x) | f_s(\overline{x})$

   (b) (1 point) $g_s(x) = f_{0^n}(x) | f_s(x)$

   (c) (3 points) $g_s(x) = f_s(x) \oplus x$

   (d) (3 points) $g_s(x) = f_x(s)$

   (e) (3 points) $g_s(x) = f_{s_1}(x) | f_{s_2}(x)$ where $s_1, s_2 \in \{0,1\}^n$ and $s = s_1 | s_2 \in \{0,1\}^{2n}$ is the concatenation of s_1 and s_2.

   (f) (4 points) $g_s(x) = f_{s_1}(x) | f_{s_2}(x)$ where $s_1 = f_s(0^n)$ and $s_2 = f_s(1^n)$.

   (g) (2 points) (extra credit) $g_s(x) = f_s(x) \oplus s$

3. *(Pseudorandom permutations (PRPs))*

   (a) (3 points) Construct a secure PRF family $\{f_s : \{0,1\}^n \to \{0,1\}^n\}_s$ where most (or even all) of the functions are *not* permutations. (You can assume that PRFs exist.)

   (b) (2 points) Based on the definition of a PRF family from class, suggest a definition of a PRP family.

   (c) (2 points) Let H be the uniform distribution over all functions $\{0,1\}^n \to \{0,1\}^n$ and let P be the uniform distribution over all permutations $\{0,1\}^n \to \{0,1\}^n$. Show that H is oracle indistinguishable from P. (Given this, can you suggest an equivalent definition in item b?)

   (d) (0 points) Given a function $f : \{0,1\}^n \to \{0,1\}^n$ (which is not necessarily a permutation) define the function $D_f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ by $D_f(L,R) = (R, f(R) \oplus L)$. This is known as the Feistel construction. Show that D_f is a permutation.

   (e) (1 point) Show that "one Feistel round" is not enough to obtain a PRP, i.e., that even if f is a PRF family, D_f need not be a PRP family.

   (f) (2 points) Show that two Feistel rounds are also not enough to obtain a PRP. Here we are referring to the family of permutation constructed by choosing $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$ independently from the PRF family, and taking $D_{f_2,f_1} : \{0,1\}^{2n} \to \{0,1\}^{2n}$ given by $D_{f_2,f_1}(x) := D_{f_2}(D_{f_1}(x))$. In class we will show that three rounds *are* enough to obtain a PRP.

[1] From Dodis

(g) (1 point) (extra credit) Show that three Feistel rounds (with the three functions chosen independently from a family of PRFs) are not enough to obtain a strong PRP. In a strong PRP the attacker is given access to both the function and its inverse.

4. (4 points) (Secret key encryption$^{\clubsuit}$) Try to give a definition of a secret key encryption scheme. Suggest one or more ways to define security for such schemes, and discuss the pros and cons of each definition. (There are many possible definitions!) Finally, propose constructions of such schemes based on cryptographic objects we have seen in class.