Homework #2

Due date & time: 10:30am on February 1, 2007. Hand in at the beginning of class (preferred), or email to the instructor (ninghui@cs.purdue.edu) by the due time.

Late Policy: Late homework will not be accepted.

Additional Instructions: (1) The submitted homework must be typed. Using Latex is recommended, but not required.

Definition 1 We call two ensembles \( \{X_n\}_{n \in \mathbb{N}} \) and \( \{Y_n\}_{n \in \mathbb{N}} \) statistical close if their statistical difference (also known as variation distance), defined as follows:

\[
\Delta(n) \overset{\text{def}}{=} \frac{1}{2} \sum_{\alpha} |\Pr[X_n = \alpha] - \Pr[Y_n = \alpha]|, 
\]

is negligible in \( n \).

Problem 1 (5 pts) An equivalent formulation of statistical closeness

Prove that two ensembles \( \{X_n\}_{n \in \mathbb{N}} \) and \( \{Y_n\}_{n \in \mathbb{N}} \) are statistically close if and only if for every set \( S \subset \{0, 1\}^* \),

\[
\Delta_S(n) \overset{\text{def}}{=} \left| \Pr[X_n \in S] - \Pr[Y_n \in S] \right|
\]

is negligible in \( n \).

Hint: Show that \( \Delta(n) \) in Definition 1 equals \( \max_S \{\Delta_S(n)\} \).

Problem 2 (5 pts) Statistical closeness implies computational indistinguishability.

Prove that if two ensembles are statistically close, then they are polynomial-time-indistinguishable.

Hint: Use the result of the previous problem, and define for every function \( f : \{0, 1\}^* \rightarrow \{0, 1\} \) a set

\( S_f \overset{\text{def}}{=} \{x : f(x) = 1\} \).

Problem 3 (10 pts) Stretching a PRNG and proof using the Hybrid Technique.

Let \( g : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1} \) be a \((t, \epsilon)\)-PRNG. Consider the function \( h : \{0, 1\}^n \rightarrow \{0, 1\}^{r+1} \) defined by

\[
h(s_0) = g(s_0) | 1 \parallel g(s_1) | 1 \parallel \cdots \parallel g(s_r) | 1,
\]

where \( 0 < r \ll 1/\epsilon \), \( s_0 \overset{\$}{\leftarrow} \{0, 1\}^n \), and \( s_i = g(s_{i-1}) | 2, \ldots, n+1 \) for \( 1 \leq r \leq r \). Then \( h \) is a \((t, \epsilon \cdot (r + 1))\)-PRNG.