Foundation of Cryptography, Spring 2013	Iftach Haitner

Problem set 1

March 19, 2013	Due: April 9

- Please submit the handout in class.
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a "solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In case you work in (small) groups, please write the id list of your partners in the solution file. I stress that each student should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appear in the first lecture (www.cs.tau.ac.il/∼iftachh/Courses/FOC/Fall11/Slides/OWF.pdf), section "Notation"

Exe 1 one way functions and P vs. NP (10 points). Prove that the existence of one-way functions implies P $\neq$ NP.

Guideline: for any poly-time computable function f define a set $L_f \in$ NP such that if $L_f \in$ P then f in insertable (by poly-time algorithm)

Exe 2 (10 points). Refute the following conjecture:

For every length-preserving one-way function f, the function $f'(x) = f(x) \oplus x$ is one-way.

Exe 3 (10 points). Let f be a one-way function. Prove that for any PPT A, it holds that

$$\mathsf{Pr}_{x \leftarrow \{0,1\}^n, i \leftarrow [n]} [\mathsf{A}(f(x), i) = x[i]] \leq 1 - \frac{1}{2n},$$

for large enough $n \in \mathbb{N}$, where $x[i]$ is the i'th bit of x.

Bonus* : prove the above when replacing $1 - \frac{1}{2n}$ with $1 - \frac{1}{n}$.

Exe 4 (basic probability). Let P and Q be distributions over a finite set $\mathcal{U}$.

a. (2 points) Prove that $\mathrm{SD}(P, Q) = \max_{\mathcal{S} \subseteq \mathcal{U}} (P(\mathcal{S}) - Q(\mathcal{S}))$ (recall that $\mathrm{SD}(P, Q) := \frac{1}{2} \sum_{u \in \mathcal{U}} |P(u) - Q(u)|$)).

b. (3 points) Prove that $\mathrm{SD}(P^2, Q^2) \leq 2 \cdot \mathrm{SD}(P, Q)$ (see "Notation" in the first class slides for the definition of P^2, Q^2).

Let $\mathcal{Q} = \{Q_n\}_{n \in \mathbb{N}}$, $\mathcal{P} = \{P_n\}_{n \in \mathbb{N}}$ and $\mathcal{R} = \{R_n\}_{n \in \mathbb{N}}$ be distribution ensembles.

c. (2 points) Given that $\mathcal{Q} \stackrel{c}{\equiv} \mathcal{P}$ (i.e., $\mathcal{Q}$ is computationally indistinguishable from $\mathcal{P}$) and $\mathcal{P} \stackrel{c}{\equiv} \mathcal{R}$, prove that $\mathcal{Q} \stackrel{c}{\equiv} \mathcal{R}$.

d. (3 points) Give an example for ensemble $\mathcal{Q}$ and $\mathcal{P}$ such that: (1) $\mathrm{Supp}(Q_n) = \mathrm{Supp}(P_n)$ for every $n \in \mathbb{N}$, and (2) $\mathrm{SD}(Q_n, P_n) = 1 - \mathrm{neg}(n)$ (i.e., for every $p \in$ poly, exists $n' \in \mathbb{N}$ with $\mathrm{SD}(Q_n, P_n) > 1 - \frac{1}{p(n)}$ for every $n > n'$)