Recall the definitions: (Definition 1 is worded slightly differently than in problem set 2 but the intention is the same.)

**Definition 1** A function $f : \mathbb{N} \rightarrow \mathbb{R}^+$ is negligible if for all $c > 0$ and all large enough $n$ we have $f(n) < 1/n^c$. (By “for all large enough $n$” we mean “there exists an $n_c$ such that for all $n > n_c$.”)

**Definition 2** Let $B : \{0,1\}^* \rightarrow \{0,1\}$ and $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be functions. We say that $B$ is a hard core predicate for $f$ if for any feasible adversary $\{A_n\}_{n \in \mathbb{N}}$ there is a negligible function $\nu$ such that for all large enough $n \in \mathbb{N}$ we have

$$\text{Prob}[x \leftarrow_R \{0,1\}^n; A_n(f(x)) = B(x)] < 1/2 + \nu(n)$$

**Question 1 (25%)**: A function is called non-negligible if there exists $c > 0$ such that for all large enough $n$ we have $f(n) > 1/n^c$. Prove or disprove: Any function is either negligible or non-negligible.

**Question 2 (25%)**: Show that any pseudorandom generator is a one way function.

**Question 3 (25%)**: Let $g : \{0,1\}^* \rightarrow \{0,1\}^*$ be a pseudorandom generator that extends its input by one bit. Define the $n$-th iteration of $g$ recursively: $g^1 = g$, and for $k > 1$ we have

$$g^{k+1}(x) = g(g^k(x)_1, ..., g^k(x)_n), g^k(x)_{n+1}, ..., g^k(x)_{n+k}.$$  

(Here $g(x)_i$ means the $i$th bit of $g(x)$.) In class we showed that if $g$ is a pseudorandom generator then so is $g^2$. Show that if $g$ is a pseudorandom generator then $g^3$ is also a pseudorandom generator.

Bonus (25%): show that $g^k$ is a pseudorandom generator for all $k$ that is polynomial in $n$. How does the allowed distinguishing probability grow as a function of $k$?

**Question 4 (20%)**: Let $B : \{0,1\}^* \rightarrow \{0,1\}$ and $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be functions. Prove or disprove: If $B$ is a hard core predicate for $f$ then $f$ is one way.

**Question 5 (30%)**: Let $B : \{0,1\}^* \rightarrow \{0,1\}$ and $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be functions. Show that $B$ is a hard core predicate for $f$ if and only if the distribution ensemble $\{f(u_n), B(u_n)\}_{n \in \mathbb{N}}$ is computationally indistinguishable from the distribution ensemble $\{f(u_n), u'_1\}_{n \in \mathbb{N}}$. (Here $u_n$ is a value chosen uniformly at random from $\{0,1\}^n$ and $u'_1$ is a value chosen uniformly at random from $\{0,1\}$, independently of $u_n$.)