1. [40 pts] (Definitions) Give a precise definition for each of the following notions.
   (a) Negligible function $\epsilon(n)$
   (b) One-way function $f : \{0,1\}^* \rightarrow \{0,1\}^*$
   (c) Pseudorandom generator $G : \{0,1\}^* \rightarrow \{0,1\}^*$
   (d) Public-key encryption scheme $(\text{Gen}, Enc, Dec)$ with message length $\ell(n)$
   (e) Non-interactive bit-commitment scheme $(\text{Com}, Ver)$.

2. [60 pts] Prove or disprove succinctly each of the following statements. If needed, you may assume that a one-way function exists or make any other (clearly stated) standard assumption.
   (a) If $f$ is a OWF then $f'(x) = f(x) \circ f(x)$ (where $\circ$ denotes string concatenation) is also a OWF.
   (b) If $G$ is a PRG then $G'(x) = G(x) \circ G(x)$ is also a PRG.
   (c) If P=NP then there is no PRG (please give a self-contained answer, without relying on any claim made in the class).
   (d) If $f$ is a OWF, then the function $P : \{0,1\}^* \rightarrow \{0,1\}$ which outputs the XOR of all of its input bits is a hardcore predicate for $f$.
   (e) If $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a pseudorandom function with key length $n$ and output length $n$, then $F'(x) = F(x, x)$ is a OWF.
   (f) If $(\text{Gen}, Enc, Dec)$ is a PKE for 1-bit messages, then the following algorithms $(\text{Com}, Ver)$ define a bit-commitment scheme: $\text{Com}(1^n, b)$ lets $(pk, sk) \leftarrow \text{Gen}(1^n)$, $c \leftarrow Enc(pk, b)$ and outputs $(com, dec)$ where $com = (pk, c)$ and $dec = sk$; $\text{Ver}(1^n, b, com, dec)$ accepts $b$ if and only if $Dec(sk, c) = b$. 