1. [30 pts] (Definitions) Give a precise definition for each of the following notions.
   (a) Negligible function $\epsilon(n)$
   (b) Computationally indistinguishable distribution ensembles $\{X_n\}, \{Y_n\}$
   (c) One-way function $f : \{0,1\}^* \rightarrow \{0,1\}^*$
   (d) Pseudorandom generator $G : \{0,1\}^* \rightarrow \{0,1\}^*$
   (e) Public-key encryption scheme $(\text{Gen, Enc, Dec})$ with message length $\ell(n)$

2. [10 pts] (Construction) Pick one of the definitions you gave in parts (c),(d), or (e) of Question 1, and describe an explicit construction which can potentially satisfy it. There is no need to prove that the construction satisfies the definition, but the construction should not be broken by the grader.

3. [42 pts] (Relations between primitives) 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) Every one-way function $f : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is a pseudorandom generator.
   (b) Every pseudorandom generator $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is a one-way function.
   (c) If $f_1, f_2$ are one-way functions, then $f(x) = f_2(f_1(x))$ is a one-way function.
   (d) If $G_1, G_2$ are pseudorandom generators, then $G(x) = G_2(G_1(x))$ is a pseudorandom generator.
   (e) If $f$ is a one-way function, then the following function $P : \{0,1\}^* \rightarrow \{0,1\}$ is a hardcore predicate for $f$. The function $P(x)$ outputs the inner product modulo 2 of the first $\lfloor |x|/2 \rfloor$ bits of $x$ and the last $\lfloor |x|/2 \rfloor$ bits of $x$.
   (f) If $F : \{0,1\}^n \times \{0,1\}^{n/2} \rightarrow \{0,1\}$ is a pseudorandom function then $F_k(x) = F(k,x)$ defines a family of collision resistant hash functions.

4. [18 pts] (Signatures)
   (a) Describe Lamport’s one-time signature scheme using a one-way function $f$.
   (b) Define a precise and meaningful notion of a “two-time signature scheme,” namely a public-key signature scheme which remains secure even if an attacker can obtain two signatures on chosen messages.
   (c) Is there a one-way function $f$ such that Lamport’s one-time signature scheme using $f$ is also a two-time signature?