1. **(Universal hash functions and hardcore predicates)** Let $H = (G,E)$, where $G$ is a PPT algorithm and $E$ is a polynomial-time algorithm. We say that $H$ is a family of universal hash functions with output length $\ell(n)$ if the following properties hold for all $n$:

- If $k$ is a possible output of $G(1^n)$ then for any $x \in \{0,1\}^n$, the output of $E(k,x)$ is of length $\ell(n)$. We denote $E(k,x)$ by $h_k(x)$.
- For any distinct $x,x' \in \{0,1\}^n$, we have $Pr_k[h_k(x) = h_k(x')] \leq 2^{-\ell(n)}$, where $k \leftarrow G(1^n)$.

Prove the following claims.

(a) For any polynomial-time computable $\ell(n)$ there is a family of universal hash functions with output length $\ell(n)$.

(b) There is a family of universal hash functions $H$ with output length $1$, such that for any one-way function $f$, the family $H$ defines a randomized hardcore predicate for $f$. (Please start your solution with a formal and self-contained definition of a “randomized hardcore predicate”.)

(c) If a one-way permutation exists, then the previous claim does not hold for every $H$. That is, there is a one-way function $f$ and a family of universal hash functions $H$ with output length $1$ such that $H$ is not a randomized hardcore predicate for $f$.

2. **(Extending the domain and range of PRFs)** Let $F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}$ be a pseudorandom function with key length $s(n)$, where $s(n)$ is a polynomial. Recall that the first argument of $F(k,a)$ is a key and the second is the input.

(a) Formally define a notion of a PRF with output length $m(n)$, and show how to use $F$ to construct such a PRF for every polynomial $m(n)$. Prove that your construction satisfies your definition.

(b) Let $0 < \epsilon < 1$ be a constant. Suppose $H = (G_H,E_H)$ is a family of universal hash functions with output length $\ell(n) \geq n^\epsilon$ and a uniformly random key of length $s'(n)$. Then $F'(k,k',a) = F(k,h_{k'}(a))$ is a PRF with key length $s'(n) + \ell(\ell(n))$, where $k$ is a random key for $F$ and $k'$ is a random key for $H$.

(c) Conclude that a PRF with key length $O(n)$ can be obtained by using a single invocation of $F$ (and no additional use of cryptography).

3. **(Constant-rate string commitment)** Recall that Naor’s bit-commitment scheme requires the sender to communicate $O(n)$ bits to the receiver. Consider the following efficient generalization, which supports commitment to an $n$-bit string with the same asymptotic communication:

- Given $n$, the receiver $R$ sends to $S$ a random string $r \in \{0,1\}^{4n}$.
- To commit to $m \in \{0,1\}^n$, the sender $S$ views $m$ as an element in the finite field $F = GF(2^n)$, views $F$ as a subfield of $\bar{F} = GF(2^{4n})$, picks a random seed $s \in \{0,1\}^n$ for a PRG $G : \{0,1\}^n \rightarrow \{0,1\}^{4n}$, and views $G(s)$ and $r$ as elements of $\bar{F}$. The commitment sent to $R$ is $c = G(s) + mr$. 
(a) Formally define a notion of an interactive, statistically binding string commitment with message length $\ell(n)$.

(b) Prove that the above protocol satisfies the definition for $\ell(n) = n$.

4. **(Rate-1 public-key encryption)** Suppose there exist a PKE and a PRG. Prove the existence of a PKE with message length $\ell(n) = n$ in which the ciphertext length is $n + o(n)$.

5. **(From an exam)** 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 $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a pseudorandom function with key length $n$ and output length $n$, then $F'(x) = F(x,x)$ is a OWF.

(b) If $(\text{Gen}, \text{Enc}, \text{Dec})$ is a PKE for 1-bit messages, then the following algorithms $(\text{Com}, \text{Ver})$ define a bit-commitment scheme: $\text{Com}(1^n, b)$ lets $(pk, sk) \leftarrow \text{Gen}(1^n)$, $c \leftarrow \text{Enc}(pk, b)$ and outputs $(\text{com}, \text{dec})$ where $\text{com} = (pk, c)$ and $\text{dec} = sk$; $\text{Ver}(1^n, b, \text{com}, \text{dec})$ accepts $b$ if and only if $\text{Dec}(sk, c) = b$. 