Problem 1: a. Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be an efficiently computable one-to-one function. Show that if $f$ has a $(t,\epsilon)$ hard core bit then $f$ is $(t,2\epsilon)$ one-way.

b. Show that if $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ is a $(t,\epsilon)$ PRNG then $G$ is also $(t',\epsilon')$ one-way for some $(t',\epsilon')$ close to $(t,\epsilon)$. Give the best bounds you can.

c. Show that if $F : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ is a $(t,\epsilon,q)$ PRF then $G(s) = F(1,s)\|F(2,s)\|\cdots\|F(q,s)$ is a $(t-q,\epsilon)$ PRNG. We are assuming that evaluating $F$ takes unit time.

Problem 2: Hybrid arguments (in part (a)).

a. Let $G : \{0,1\}^n \rightarrow \{0,1\}^m$ be a $(t,\epsilon)$ PRNG. Define the distributions $P_1$ and $P_2$ as:

$$P_1 = \{G(x_1),\ldots,G(x_q) \in \{0,1\}^m \mid x_1,\ldots,x_q \leftarrow \{0,1\}^n\}$$

$$P_2 = \{y_1,\ldots,y_q \leftarrow \{0,1\}^m\}$$

Show that $P_1$ and $P_2$ are $(t-cq,q\epsilon)$ indistinguishable for some constant $c > 0$.

b. Let $H$ be a group of prime order $q$ and $g \in H$ a fixed public generator. Consider the following PRNG, $G : \mathbb{Z}_q^2 \rightarrow H^3$, defined by $G(a,b) = [g^a, g^b, g^{ab}]$. As above, define the two distributions:

$$P_1 = \{G(a_1,b_1),\ldots,G(a_q,b_q) \in H^3 \mid a_1,b_1,\ldots,a_q,b_q \leftarrow \mathbb{Z}_q\}$$

$$P_2 = \{h_1,\ldots,h_{3q} \leftarrow H\}$$

Show that if the $(t,\epsilon)$-DDH assumption holds in $H$ then $P_1$ and $P_2$ are $(t-cq,\epsilon)$ indistinguishable for some constant $c > 0$ (assuming exponentiation in $H$ takes constant time). Hence, for DDH PRNG we get a more efficient reduction than for general PRNG’s.

Problem 3: In this problem we develop a simple version of the Goldreich-Levin algorithm. Suppose $\alpha \in \{0,1\}^n$ and $f_\alpha : \{0,1\}^n \rightarrow \{0,1\}$ is an oracle satisfying

$$\Pr[f_\alpha(x) = x \cdot \alpha] > \frac{3}{4} + \epsilon$$

where $x \cdot \alpha$ is the inner product modulo 2 of $x$ and $\alpha$. Show that $\alpha$ can be recovered from the oracle $f$ with probability 1/2 by making $O(n/\epsilon)$ oracle queries.

Hint: Show that the first bit of $\alpha$ can be found by querying $f_\alpha$ at many pairs of points $(r_1 r_2 \ldots r_n, \bar{r}_1 r_2 \ldots r_n)$. Generalize to show that all bits of $\alpha$ can be found. Use the Chernoff bound to bound the success probability of your algorithm.

Remark: This approach can be extended to reduce the $\frac{3}{4} + \epsilon$ bound to $\frac{1}{2} + \epsilon$. The extension is based on making the query points pair wise independent rather than completely independent.
**Problem 4:** Let $F : \{0,1\}^n \times \{0,1\}^s \rightarrow \{0,1\}^t$ be a $(t, \epsilon, q)$ unpredictable function (UF). For vectors $x, y \in \{0,1\}^t$ define $x \cdot y$ to be the inner product of $x$ and $y$ modulo 2, i.e. $x \cdot y = \sum_{i=1}^{n} x_i y_i \mod 2$. Define the function $F' : \{0,1\}^n \times \{0,1\}^{s+t} \rightarrow \{0,1\}$ by

$$F'_{k,r}(x) = F'(x, (k, r)) \overset{\text{def}}{=} F_k(x) \cdot r \in \{0,1\}$$

Prove using the Goldreich-Levin algorithm that $F'$ is a $(t', \epsilon', q')$-PRF for some $t', \epsilon', q'$. Give the best parameters $t', \epsilon', q'$ you can.

As a simple application for this result, note that your proof suggests one way for converting any deterministic MAC into a symmetric encryption scheme.

**Problem 5:** Let $H = \{h_k : \{0,1\}^N \rightarrow \{0,1\}^n\}$ be a family of hash functions such that

$$\forall x \neq y \in \{0,1\}^N : \Pr_{h \leftarrow H}[h(x) = h(y)] < \epsilon'.$$

Let $F : \{0,1\}^n \times \{0,1\}^s \rightarrow \{0,1\}^t$ be a $(t, \epsilon, q)$-PRF.

Prove that $HF_{k_1,k_2}(M) = F_{k_1}(h_{k_2}(M))$ is a $(t, \epsilon + \epsilon', q)$ unpredictable function (UF).

**Problem 6:** Let $\pi : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ be a $(t, \epsilon, q)$ PRP. Given $k$, both $\pi_k(x)$ and $\pi_k^{-1}(x)$ can be efficiently computed. Show how to construct an SPRP out of $\pi$. Prove that your construction is a $(t', \epsilon', q)$ SPRP. Give the best values of $t', \epsilon'$ you can. Your solution suggests a way of converting any block cipher that is resistant to chosen PT attacks into a block cipher that resists both chosen PT and chosen CT attacks.