Problem Set 3

1. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a (t,ϵ)-secure pseudorandom generator computable in time r.

   Show that G is also a $(t - r - O(n), \epsilon + 2^{-n})$-secure one way function.

2. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a (t,ϵ)-secure one-way function.

   Show that

   $$\frac{t}{\epsilon} \leq O((m+n) \cdot 2^n)$$

3. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a (t,ϵ)-secure one-way permutation computable in time $\leq r$.

   Show that

   $$\frac{t^2}{\epsilon} \leq O((r+n^2)^2 \cdot 2^n)$$

   [Hint: first show that, for any permutation $f : \{0,1\}^n \to \{0,1\}^n$, there is an algorithm of complexity $O(r \cdot 2^{n/2})$ that inverts the permutation everywhere. The algorithm is given a pre-computed data structure of size $O(n2^{n/2})$ and runs in time $O(r2^{n/2})$. Recall that in our model of computation we do not pay for the price of pre-computing data at "compile time," we only pay the sum of the length of the program, including any fixed data it needs access to, plus the worst-case running time.]

4. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a (t,ϵ)-secure one-way function computable in time r.

   Show that $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined as $g(x,y) := f(x), f(y)$ is $(t - O(r), \epsilon)$-secure.

5. Let p be a prime and g be a generator for $\mathbb{Z}_p^*$ such that $f(x) := g^x \bmod p$ is a $(t, 0.99)$-one way permutation. Let $k = \lceil \log_2 p \rceil$ be the number of digits of p; then recall that $f()$ is computable in time $O(k^3)$.

   Show that $f()$ is also $(\frac{1}{24{,}000}(t - O(k^3)), 0.51)$-one way.

6. Recall that if $F : \{0,1\}^n \to \{0,1\}^n$ is a function then the we define the Feistel permutation $D_F(x, y) := y, x \oplus F(y)$.

   Show that there is an efficient oracle algorithm A such that

$$\mathop{\mathbb{P}}_{\Pi:\{0,1\}^{2m}\to\{0,1\}^{2m}}[A^{\Pi,\Pi^{-1}} = 1] = 2^{-\Omega(m)}$$

   where Π is a random permutation, but for every three functions F_1, F_2, F_3, if we define $P(x) := D_{F_3}(D_{F_2}(D_{F_1}(x)))$ we have

$$A^{P,P^{-1}} = 1$$

   [Note: I don't know the solution.]