Assignment 4

Policy: You may discuss problems with others, but all written work submitted must be your own. *You may not copy nor solicit solutions, complete or partial, from any source.*

Notes: log will refer to $\log_2$.

"One-way function" refers to "*strong* one-way function."

1. Show that the following probability ensembles X_n on $\{0,1\}^n$ fail the next bit test:
   - For each n, the first $n-1$ bits are uniformly random, and the last bit is the sum of the first $n-1$ bits mod 2.
   - For each n, the bits are uniformly random, unless there have been $\lceil 5\log(n)\rceil$ 0s in a row. In this case, the next bit is always 1.
   - (Optional, not for credit) What if I replaced $\lceil 5\log(n)\rceil$ with $\lceil 5\sqrt{n}\rceil$ above?
2. Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a pseudorandom generator. Show that G is a one-way function. (You may want to first assume that G is one-to-one and see what result you can get. Then try to drop this assumption.)
3. Let $f : \{0,1\}^* \to \{0,1\}^*$ be an efficiently computable one-to-one function with a hardcore bit $h(x)$. Show that f is a one-way function.
4. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a one-way function, and let $h(s)$ be a hard-core bit for f. Define $G(s) = f(s)||h(s)$. Show that G is not necessarily a pseudorandom generator. (Note the slight difference in wording with 79.4!)
5. (Extra credit) Do the following, using whatever programming language you'd like. You will be producing a pseudorandom list of bits, using the least significant bit of RSA as a hardcore bit.
   - Let p be a random prime between 100 and 1000.
   - Let q be a random prime 100 and 1000. If $q = p$, pick a different one.
   - Set $N = pq$, and $M = (p-1)(q-1)$.
   - Let e be a random integer from 3 to M. If $gcd(e, M) \neq 1$, pick a different e. Keep doing so until $gcd(e, M) = 1$.
   - Let x be a random integer from 2 to N. If $gcd(x, N) \neq 1$, pick a different x. Keep doing so until $gcd(x, N) = 1$.

- Using some type of loop, produce the string of bits $b_1 b_2 \dots b_{200}$, where

$$y_1 = x, \qquad b_1 = y_1 \mod 2;$$

  And for $i \geq 1$,

$$y_{i+1} = (y_i^e \mod N); \qquad b_{i+1} = y_{i+1} \mod 2$$

- Share p, q, e, and the string of 200 bits in a readable format (and we'll have a place to submit your code). Does the sequence appear to be random?

6. (Optional, not for credit) Prove that if a one-way function exists, then there exists a one-way function $f : \{0,1\}^n \to \{0,1\}^*$ such that for all i from 1 to n, there is an adversary A_i such that

$$P[x \leftarrow \{0,1\}^n; y = f(x) : A_i(1^n, y) = x_i] \geq \frac{1}{2} + \frac{1}{2n},$$

   where x_i is the ith bit of x. That is, no single bit of x is a hard-core bit for f.