Assignment 2

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.*

log will refer to $\log_2$.

1. Show using Definition 27.2 that
   (a) $\epsilon(n) = n^{-\log\log n}$ is a negligible function. How large does n need to be before $\epsilon(n) \leq n^{-100}$?
   (b) If $\epsilon(n)$ is a negligible function, and n^r is a polynomial, then $n^r\epsilon(n)$ is also a negligible function.
   (c)
   $$f(n) = \begin{cases} 1/n^{99} & \text{if n is prime} \\ 2^{-n} & \text{otherwise} \end{cases}$$
   is NOT a negligible function.

2. Suppose that $f : \{0,1\}^* \to \{0,1\}^*$ is such that $|f(x)| < c\log(|x|)$ for every $x \in \{0,1\}^*$, where $c > 0$ is some fixed constant. (Here $|\cdot|$ denotes the length of a string.) Prove that f is not a strong one-way function.

3. Suppose we have an efficiently computable function $f : \{0,1\}^* \to \{0,1\}^*$ such that for any adversary $\mathcal{A}$ and all n,
   $$P[x \leftarrow \Pi_n; y \leftarrow f(x) : f(\mathcal{A}(1^n, f(x))) = y] < e^{-n}.$$
   Note that x is being sampled from the set of n-bit *primes*. Show that f is a weak one-way function.

4. Prove that if $f : \{0,1\}^n \to \{0,1\}^*$ is a strong one-way function, then the function $g : \{0,1\}^{2n} \to \{0,1\}^*$ defined by $g(x_1, x_2) = (x_1, f(x_2))$, is a strong one-way function.

5. Explain why it is the case that when algorithm A' (Algorithm 33.6) uses A as a subroutine, A does indeed receive the product of two uniformly distributed n-bit integers, assuming that A' received the product of two uniformly random n-bit primes.

6. (Based on the discussion on page 34) Justify the comment that this modified algorithm A'' succeeds in factoring with at least the same if not greater probability than A'.

7. Suppose we repeatedly and independently pick a random n-bit integer until we find one that is prime. Let X be the number of times we have to sample before successfully finding a prime (assume we do prime-checking in a deterministic way).

   (a) What type of distribution does the random variable X have?

   (b) Find an upper bound on $E[X]$.

   (c) Find an upper bound on $P[X > m]$. Find a function $m(n)$ that makes this upper bound a negligible function of n.