Homework 24, due November 1

(1) Consider the following hash function. Let n be a large integer. Messages are in the form of a sequence of integers $(a_1, a_2, \ldots, a_s)$, where each a_i satisfies $0 \leq a_i < n$. The hash function h is computed as $a_1 + a_2 + \ldots + a_s \pmod{n}$. Which of the requirements for a good hash function from section 8.1 are satisfied by h? Explain.

(2) (Page 239, problem 2) Let $n = pq$ be the product of two distinct large primes and let $h(x) = x^2 \pmod{n}$. Why is h preimage resistant? (There are some values, like $1, 4, 9, 16, \ldots$, for which finding a preimage is easy. But usually it is difficult.) Why is h not collision-resistant?

(3) (a) Let H be the hash function defined by $H(m) = m$. Show that H has second pre-image resistance but not pre-image resistance.

(b) Show that if a hash function H is collision-resistant, then it has second pre-image resistance. (Hint: prove the contrapositive.)