Homework 27, due November 6

(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 strongly collision-free?

(3) Let h be a hash function whose input is a string of letters, spaces, and punctuation, and whose output is an integer $\pmod{100}$. Use the 100 character alphabet (ASCII - 32) used earlier. The function h adds together the numerical representation of each character in the string and outputs the result $\pmod{100}$. For example, the string "Hello." would have output $h(Hello.) = 40+69+76+76+79+14 \pmod{100} = 54$. By trying a number of good and bad messages, find two messages with the same hash, one of which you could convince someone to sign (for example, "Go BYU") and one which they would refuse to sign (for example, "I will pay you ten dollars"). (You will use the result of this problem in problem 1 of HW 29.)