Homework 19, due November 10

(1) (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?

(2) 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 20.)

(3) In a family of six, what is the probability that no two people have birthdays in the same month? Assume that all months have equal probabilities.

(4) (Page 242, problem 1)
   (a) If there are 30 people in a room, what is the probability that at least two have the same birthday? Compare this to the approximation in formula (8.1).
   (b) How many people should there be in a room in order to have a 99 percent chance that at least two have the same birthday?
   (c) How many people should there be in a room in order to have a 100 percent chance that at least two have the same birthday?