IS2935/TEL 2810 Introduction to Computer Security
Homework 7
Due Date: November 11, 2004
(100 Points)

The following property of modular arithmetic will be helpful in solving some problems

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
- $(-1) \bmod n = n - 1$ (Using $b = q.n + r$, with $b = -1$, $q = -1$ and $r = n-1$)

9.8.11 (We did this in class!!)
9.8.13 (For n-1 case, you could use induction and the properties of modular arithmetic)
10.10.8 (Hint: use the properties above).