HW 10 CMSC 389. DUE Jan 19

1. (0 points) READ my NOTES on RSA and SECRET SHARING- PARTICULARLY SHORT SHARES.

2. (40 points) (In this problem we outline how you can have a finite field of 4 elements.) Let $F = \{0, 1, x, x+1\}$. The coefficients are in mod 2, so $x + x = 2x = 0x = 0$. Multiplication will be such that whenever you multiply two numbers you replace any term of the form x^2 with $x + 1$.

   (a) Form the addition table for F. You need not tell us what 0 plus stuff is since $0 + blah = blah$. You can assume addition is commutative so you don't have to tell us both $a + b$ and $b + a$.

   (b) For every element in F say what its additive inverse is.

   (c) Form the mult table for F. You need not tell us what 1 times stuff is since $1 \times blah = blah$. You need not tell us what 0 times stuff is since $0 \times blah = 0$. You can assume mult is commutative so you don't have to tell us both ab and ba.

   (d) For every NONZERO element in F say what its mult inverse is.

3. (60 points) In the notes and class I told you how to, using RSA, have a secret sharing scheme where every share was $2|s|/t$. In the notes (and maybe in class- I am writing this before I gave class) I gave a scheme where you use two polys for the encoded secrete and one for the key that used shares of size $3|s|/t$.

   (a) Describe rigorously the scheme where you use three polys for the encoded secrete and one for the key. How short are the shares?

   (b) Describe rigorously the scheme where you use L polys for the encoded secrete and one for the key. How short are the shares?

   (c) Is there a limit to how many polys you should use?