HW 11, Due Jan 20

READ THE NOTES ON SECRET SHARING
READ THE NOTES ON FINDING INVERSES
THIS HW IS TWO PAGES LONG!!!!!!

1. (40 points) We have used the following:

   t points determine a $t-1$ degree poly, but $t-1$ points DO NOT DETERMINE ANYTHING!!!

   We have used this over mod p for p prime.

   You probably know the following:

   3 points in determine a plane but 2 points DO NOT DETERMINE ANYTHING!!!

   YOU GUESSED IT!- This is true mod p for p prime.

   NOTE: We can assume planes are of the form $x + by + cz = d$ since if we have $ax + by + cz = d$ we can multiply by a^{-1}. (a^{-1} CAN BE FOUND FAST- READ NOTES ON IT.)

   (a) You are told that a plane in mod 7 has points $(1, 1, 1)$, $(2, 2, 3)$, $(3, 3, 1)$. What is the equation of the plane?
   (EQ1) $1 + b + c = d$
   (EQ2) $2 + 2b + 3c = d$
   (EQ3) $3 + 3b + c = d$
   By EQ1 and EQ3 we have
   $1 + b + c = d = 3 + 3b + c$
   $1 + b = 3 + 3b$
   $2b = -2$ so $b = -1 = 6$.
   EQ1 now gives $c = d$.
   EQ2 now gives $2 + 2 \times 6 + 3c = c$
   $3c = c$
   $2c = 0$
   $c = 0$. So we have $d = 0$.
   SO we have $b = 6$, $c = 0$, $d = 0$ so the plane is

$$x + 6y = 0$$

(b) Devise a secret sharing scheme that has all of the following properties:

- Zelda has 100 friends named $A_1, \ldots, A_{100}$,
- Zelda has a secret s
- p is the smallest primes such that $s \in \{0, 1, \ldots, p-1\}$,
- Zelda wants that if THREE of her friends get together then they can decode the secret, but if two get together they cannot,
- the scheme should use the following: *three points in* $\{0, \ldots, p-1\}$ *mod* p *determine a plane but two points do not determine anything*
- the strings given to all participants are roughly $|s|$ long.
- the scheme is information-theoretic secure.

Recall that the equation of a plane in 3-dim space is $ax+by+cz = d$. We rewrite this as $z = (d - ax - by)c^{-1}$ where c^{-1} means c inverse in mod p.

Zelda does the following: pick RANDOM numbers $a, b, c \in \{0, \ldots, p-1\}$. Let $f(x, y) = (d - ax - by)c^{-1}$.

Give A_1 the value $f(1, 1)$

Give A_2 the value $f(2, 2)$

etc.

If three of them get together than they have three points on the plane, so they can determine the plane and hence s.

TO modify so that get shorter strings do trick similar to PUBLIC KEY trick.

2. (60 points) RECALL: In class I went over the method of *secret sharing with shorter shares* where everyone gets a share of size $|PUB| + |k| + |s_i| = 3|s|/t$. This involved two polynomials: $f(x)$ which had $ENC(s_i, PUB)$ as coefficients and $g(x)$ which had k as its constant term. I then suggested two ways to shorten the share even more. In this problem you will extend both methods.

   (a) RECALL METHOD ONE: I split the key k into t pieces, used an encoding of it which involved another (shorter) key. EXTEND

THIS to 3 levels. How long is each share? Then to L levels. How long is each share? For which L does the method not work?

(b) RECALL METHOD TWO: I spit s into $2t$ pieces. EXTEND THIS to $3t$ pieces. How long is each share? EXTEND THIS to Lt pieces. How long is each share? For which L does the method not work?

a) The secret is split into t pieces $s = s_0 \cdots s_{t-1}$. A key k is picked for an Public Key system, and PUB is picked Let $E(s_i, k, PUB) = u_i$. NOTE that $|u_i| = |k| = |PUB| = |s_i| = |s|/t$.

Let

$$f(x) = u_{t-1}x^{t-1} + \cdots + u_0$$

NOTE: For all j, $|f(j)| = |s|/t$.

We now split up the key itself. Let $k = k_0 \cdots k_{t-1}$. A key k' is picked for an Public Key system, and PUB' is picked Let $E(k_i, k', PUB') = v_i$. NOTE that $|v_i| = |k_i| = |PUB'| = |k_i| = |k|/t = |s|/t^2$.

Let

$$g(x) = v_{t-1}x^{t-1} + \cdots + v_0$$

NOTE: For all j, $|g(j)| = |s|/t^2$.

Zelda picks $a_1, \ldots, a_{t-1}$ at random. Let

$$h(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + k'$$

Zelda gives A_i the following: $f(i)$, $g(i)$, $h(i)$, PUB, PUB'

Thats of length

$$|s|/t + |s|/t^2 + |s|/t^2 + |s|/t + |s|/t^2 = 2|s|/t + 3|s|/t^2$$

We leave the case of L iterations to you.

b) The secret is split into $3t$ pieces:

$$s = s_0^1 s_1^1 s_2^1 \cdots s_{t-1}^1 s_0^2 s_1^2 s_2^2 \cdots s_{t-1}^2 s_0^3 s_1^2 s_2^3 \cdots s_{t-1}^3$$

Note that $|s_i^j| = |s|/3t$. A key k is picked for an Public Key system, and PUB is picked Let $E(s_i^j, k, PUB) = u_i^j$. NOTE that $|u_i^j| = |k| = |PUB| = |s_i| = |s|/3t$.

Let

$$f_1(x) = u_{t-1}^1 x^{t-1} + \cdots + u_0^1$$

$$f_2(x) = u_{t-1}^2 x^{t-1} + \cdots + u_0^2$$

$$f_2(x) = u_{t-1}^3 x^{t-1} + \cdots + u_0^3$$

A key k is picked for an Public Key system, and PUB is picked Zelda picks $a_1, \ldots, a_{t-1}$ at random. Let

$$h(x) = a_{t-1} x^{t-1} + \cdots + a_1 x + k$$

Zelda gives A_i the following: $f_(i), f_2(i), f_3(i), h(i)$, PUB

Thats of length

$$|s|/3t + |s|/3t + |s|/3t + |s|/3t + |s|/3t = 5|s|/3t$$

We leave the case of L iterations to you.