HW 10, Due Jan 19

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

1. (30 points) Zelda has a secret that is an elements of $\{0, 1, 2, \ldots, 12\}$. She will use mod 13 to share it. She wants it to be the case that if three people get together then they can crack it, but two people cannot. She uses the polynomial method.

   (a) If Zelda gives A_1 the value 8 and A_2 the value 11 and A_3 4 then what is the secret?

   (b) Is it possible that Zelda gives A_1 the value 1, A_2 the value 4 and A_3 the value 9 and A_4 the value 1? If YES then give the secret. If NOT then why not?

   (c) Is it possible that Zelda gives A_1 the value 1, A_2 the value 4 and A_3 the value 9 and A_4 the value 2? If YES then give the secret. If NOT then why not?

2. (30 points) Zelda has a secret that is an elements of $\{0, 1, 2, \ldots, 63\}$. Notice that the secret is a 6-bit string. She will use mod 67 to share it. (NOTE- you can use WOLFRAM ALPHA to find inverses mod 67.) She wants it to be the case that if three people get together then they can crack it, but if two get together they cannot.

   (a) Zelda does the usual poly-secret sharing where the constant is the secret. She gives A_1 the value 1, A_2 the value 2, and A_3 the value 4. What is the secret?

   (b) Zelda does the really stupid thing of splitting the 6-bit secret into three parts and using a polynomial that has those three parts as coefficients. The parts are all 2-bits long so the max coefficient is 3. She uses mod 5. She gives A_1 the value 4, A_2 the value 2, and A_3 the value 4. What is the secret?

   SOLUTION TO 2b.

   ALL arithmetic is in the finite field on 2^6 elements.

   The secret is $s = s_0s_1s_2s_3s_4s_5$. The s_i's are bits.

Contract:

Shamir Secret Sharing: Zelda picks random a_2, a_1 that are in $\{0, \ldots, 63\}$ and forms the polynomial

$$f(x) = a_2x^2 + a_1x + s.$$

and give A_i $f(i)$. Note that A_1 gets $a_2 + a_1 + s$. Since a_1, a_2 are random this yields NO information

The coefficients are of length 6.

Stupid way: use

$$g(x) = s_5s_4x^2 + s_3s_2x + s_1s_0$$

and give A_i $f(i)$. Note that A_1 gets

$$s_5s_4 + s_3s_2 + s_1s_0.$$

THIS IS INFORMATION!!! Having this number cuts down on the possible secrets. For example, if this number is 0 then the secret cannot be 000001.

END OF SOLUTION TO 2b

3. (20 points) Zelda has a secret. She has 100 friends named $A_1, \ldots, A_{100}$. She wants it to be the case that, for all $1 \le i \le 98$, if A_i, A_{i+1}, A_{i+2} get together then they can find the secret and of course all supersets of those sets, but no other sets.

   (a) If she does this by the random string method then, for each $1 \le i \le 100$, how many strings does A_i get. (It may be different for different i.)

   (b) What is the total number of strings that Zelda sends out?

   (c) (Just think about, no points) Is there a method that leads to LESS strings being send out?

4. (20 points) Zelda wants to do the polynomial method over mod 100. Why is this a terrible idea. be COHERENT, CLEAR, and CONCISE.

   SOLUTION TO 4

   Assume Zelda uses the poly method over mod 100. When Alice and Bob and Carol try to interpolate the polynomial then will need to TAKE INVERSES! There will be cases where they can't do this and hence cannot recover the secret!!!

   END OF SOLUTION TO 4