HW 9 CMSC 389. DUE Jan 18
SOLUTIONS
THIS HW IS TWO PAGES!!!!!!!!!!!!!!!!

1. (0 points) READ my NOTES on RSA and SECRET SHARING

2. (20 points) (In this problem you can leave an answer in terms of factorials and powers and not multiply it out.) Assume n is even. Zelda wants to share a secret s with $A_1, \ldots, A_n$ so that any $n/2$ of them can recover the secret, but no $n/2 - 1$ can.

   (a) If she uses the Random String Method then how many strings of length $|s|$ does each A_i get? Explain your answer.

   (b) If she uses the Polynomial Method then how many strings of length $|s|$ does each A_i get? Explain your answer.

   SOLUTION TO PROBLEM 2

   2a) Fix i. For every subset of $\{1, 2, \ldots, n\}$ of size $n/2$ that includes i, A_i gets a string of length $|s|$. How many such sets are there? This is equivalent to the number of subsets of size $n/2-1$ of $\{1, 2, \ldots, i-1, i+1, \ldots, n\}$, which is $\binom{n-1}{(n/2)-1}$.

   NOTE: If you wrote $\binom{n}{n/2}$ you got 5 points.

   2b) With the poly method A_i just gets $f(i)$, ONE string of length $|s|$.

3. (20 points) Let $f(x) = ax^2+bx+c \pmod{11}$. We are told that $f(1) = 2$, $f(2) = 4$, and $f(3) = 8$. Find a, b, c.

   SOLUTION TO PROBLEM 3

   (We essentially follow Theorem 5.5 in the secret sharing notes. Most people did it by solving a system of linear equations which is fine so long as they make sure its all in mod 11. So NO 1/3 or -4. If you had a negative value anywhere then you lost 5 points.)

$$h_1(x) = 2\frac{x-2}{1-2}\frac{x-3}{1-3}$$

   (This is slightly diff then the notes.)

We need to NOT use those denominators- we need to make them numbers in mod 11.

$\frac{1}{1-2} = \frac{1}{-1} = \frac{1}{10} = 10$ (since $10 \times 10 \equiv 1$).

$\frac{1}{1-3} = \frac{1}{-2} = \frac{1}{9} = 5$ (since $9 \times 5 \equiv 1$).

So we have

$$h_1(x) = 2 \times 10(x-2) \times 5(x-3)$$

$$= 100(x-2)(x-3) = (x-2)(x-3) = x^2 - 5x + 6 = x^2 + 6x + 6$$

Note that

$h_1(1) = 2$

$h_1(2) = 0$

$h_1(3) = 0.$

We now get h_2

$$h_2(x) = 4\frac{x-1}{2-1}\frac{x-3}{2-3}$$

$\frac{1}{2-1} = \frac{1}{1} = 1$

$\frac{1}{2-3} = \frac{1}{-1} = 10.$

$$h_2(x) = 4(x-1)10(x-3) = 40(x-1)(x-3)$$

$$= 7(x-1)(x-3) = 7(x^2 - 4x + 3) = 7(x^2 + 7x + 3)$$

$$= 7x^2 + 49x + 21 = 7x^2 + 5x + 10$$

We now get h_3

$$h_3(x) = 8\frac{x-1}{3-1}\frac{x-2}{3-2}$$

$$\frac{1}{3-1} = \frac{1}{2} = 6$$

$\frac{1}{3-2} = \frac{1}{1} = 1$.

$$h_3(x) = 8 \times 6(x-1)(x-2) = 48(x-1)(x-2)$$

$$= 4(x^2 - 3x + 2) = 4(x^2 + 8x + 2)$$

$$= 4x^2 + 32x + 8 = 4x^2 + 10x + 8$$

We add all of these up

$$h_1(x) + h_2(x) + h_3(x)$$

$$= x^2 + 6x + 6 + 7x^2 + 5x + 10 + 4x^2 + 10x + 8$$

$$= (1 + 7 + 4)x^2 + (6 + 5 + 10)x + (6 + 10 + 8)$$

$$= x^2 + 10x + 2$$

4. (20 points) For each of the following secrets say the smallest field that can be used to share the secret and explain why. (RECALL- there are fields of size every prime power. We use the ones of size power-of-two.)

   (a) $s = 15$

   (b) $s = 16$

   (c) $s = 17$

   (d) $s = 18$

SOLUTION TO PROBLEM 4

There are fields of any prime power size.

$s = 15 = (1111)_2$. So this will need a field that has 4-bit strings as elements. Use the field on 16 elements.

$s = 16 = (10000)_2$. So this will need a field that has 5-bit strings. You COULD use the field of mod 19. But then the players will know that its one of the few 5-bit strings in the field so some information is leaked. So you need to use the field on 32 elements. (Even so, this was graded as correct.)

$s = 17 = (10001)_2$. So this will need a field that has 5-bit strings. So you need to use the field on 32 elements.

$s = 18 = (10010)_2$. So this will need a field that has 5-bit strings. So you need to use the field on 32 elements.

THERE IS A SECOND PAGE!!!!!!!!!!!!

5. (20 points) Zelda has a secret $s = 7$. Note that $7 = (111)_2$ so it takes 3 bits (formally we would need to use the Field on 2^3 elements but in this problem we will use the (easier to work with) mod field of 11 elements). that she wants to share with $A_1, \ldots, A_{10}$ such that if 3 of them get together they can find out the secret but if 2 of them get together they cannot. She wants to give everyone one share in $\{0, \ldots, 10\}$. She will use the polynomial method over mod 11. Recall that she gives A_i $f(i)$.

   (a) If we know that A_1 has 1 and A_2 has 2 then can we determine the secret? If so then say how, if not then say why not.

   (b) If we know that A_1 has 2 and A_2 has 3 and A_3 has 4 then can we determine the secret? If so then say how, if not then say why not.

   (c) If we know that A_1 has 1 and A_2 has 2 and A_3 has 4 then can we determine the secret? If so then say how, if not then say why not.

   SOLUTION TO PROBLEM 5

   5a) NO. A_1 and A_2 have two points of a quadratic so they cannot determine it.

   5b) YES. Since its a quadratic and we have three points we can determine it. In fact this one is easy: since $f(1) = 2$, $f(2) = 3$, and $f(3) = 4$ we already know that $f(x) = x + 1$ works. Any quadratic that agrees with this f would have to BE this f. The constant term is 1, so the secret is 1.

   5c) YES. Since its a quadratic and we have three points we can determine it. We leave the interpolation (the h_j stuff) to you.

6. (20 points) The version of RSA I gave you in class left out an important point (intentionally so I could ask this question on this exam). Below I give the first step of RSA I did in class but I italicize a problem with it and then ask a question about it.

   - Alice picks random primes p, q. *She then finds a number* $e \in \{1, \ldots, (p-1)(q-1)\}$ *such that* e *is relatively prime to* $(p-1)(q-1)$. She then finds a $d \in \{1, \ldots, (p-1)(q-1), -1\}$ such that $ed \equiv 1 \pmod{(p-1)(q-1)}$ (such exists since e is rel prime to $(p-1)(q-1)$. She computes $n = pq$ and broadcasts $(n, d, SOTE)$.

In Step 1 I never said how she could find a number e that is rel prime to $(p-1)(q-1)$. How can she modify step 1 so that she can find such a e quickly? Two warnings:

- Picking e prime won't help— if $p = 101$, $q = 103$, and $e = 5$ then note that 5 is NOT rel prime to $100 * 102$.
- DO NOT do *pick an e, test if, it works great, if not then try again* as this might take too long if you keep getting e's that do not work.

SOLUTION TO PROBLEM 5

This is similar to when we said about Diffie-Helman:

we have to factor $p-1$? But factoring is hard!

In that case rather than factor it we found primes p such that $p-1$ came already factored- safe primes.

We do the same here:

(a) Alice generates Safe Primes p, q. Let $p-1 = 2p'$ and $q-1 = 2q'$ where p', q' are primes. Then

$$(p-1)(q-1) = 4p'q'$$

(b) Generate a random $e \in \{(p-1)(q-1)/3, \ldots, 2(p-1)(q-1)/3\}$. Test if any of $2, p', q'$ divide e. If not then output e. If yes than try again.

Very few numbers have 2, p', q' dividing it, so you will find an e quickly. Lets be more precise.

$\phi(4pq) = 2(p-1)(q-1)$, so the prob of hitting a good e is $1/2$.

Did we have to pick such a p, q. YES and NO. If we picked a random p, q then there IS a way to test of e is rel prime to $(p-1)(q-1)$ without factoring $(p-1)(q-1)$. But if $(p-1)(q-1)$ has a lot of factors then you may need to try a lot of e's until you find one.

Example: If $p = 31$ and $q = 43$ then $(p-1)(q-1) = 30 \times 42 = 2 \times 3 \times 5 \times 2 \times 3 \times 7 = 2^2 \times 3^2 \times 5 \times 7$

Note that

$$\phi(p-1)(q-1)) = \phi(2^2 \times 3^2 \times 5 \times 7) =$$

$$= (2^2 - 2)(3^2 - 3)(4)(6) = 2 \times 6 \times 2^2 \times 2 \times 3 = 2^5 \times 3^2 \times$$

Hence the probability of hitting a number that is rel prime is

$$\frac{2^5 \times 3^2}{2^2 \times 3^2 \times 5 \times 7}$$

$$= \frac{2^3}{5 \times 7} = \frac{8}{35}$$

This is less than 1/4, not as good as 1/2. And it can get worse.

NOTE: Some solution involved special types of primes. That was fine also.