HW 9 CMSC 389. DUE Jan 18
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.

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.

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) $s = 18$

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.

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.