## HW 5 CMSC 389. DUE Jan 18
## THIS HW IS THREE PAGES!!!!!!!!!!!!!!!!

1. (0 points) READ the NOTES on SECRET SHARING

2. (30 points) Assume there is already a fast procedure to TEST if a number is prime. Call it TEST(n).

   (a) (15 points) Write psuedocode for an algorithm that, on input $N$, finds a SAFE prime between $N$ and $2N$ and SKIPS any number $n$ that is divisible by 2, 3, or 5.

   (b) (15 points) In your code for Part 1 you should have tested if $(n-1)/2$ was prime to ensure that $n$ was a safe prime. You may have ended up testing numbers of this form that are divisible by 2,3, or 5. SO lets make it faster: Write pseudocode for an algorithm that, on input $N$, finds a SAFE prime between $N$ and $2N$ and SKIPS at any number $n$ such that $n$ is divisible by 2, 3, or 5 OR such that $(n-1)/2$ is divisible by 2, 3, or 5.

3. (OPTIONAL) Zelda wants to share a secret $s$ with $A_1, \ldots, A_{n+1}$ so that

   - $A_1$ and $A_2$ can determine the secret,
   - $A_2$ and $A_3$ can determine the secret,
   - $A_3$ and $A_4$ can determine the secret,
   - $\vdots$
   - $A_n$ and $A_{n+1}$ can determine the secret.

   Zelda uses the Random String Method.

   (a) Explain what Zelda does.

   (b) For any particular $i \in \{1, \ldots, n+1\}$ how many random strings does $A_i$ get?

**GO TO NEXT PAGE!**

4. (OPTIONAL) Zelda has a secret $s$ in the integers mod 13 and she wants to give shares to $A_1, \ldots, A_{10}$ such that

   - If $A_1, A_2$ and ANY three of $\{A_3, \ldots, A_{10}\}$ get together then they can find out the secret, but NO two can.
   - Each person gets ONE string of length $s$.
   - The scheme is information-theoretic secure.

   Explain how Zelda can do this.

5. (40 points) Zelda has a secret and she wants to use the polynomial method over mod 17. She wants to share it with $A_1, \ldots, A_6$ such that if 4 of them get together they can find out the secret but if 3 of them get together they cannot. She wants to give everyone one share in $\{0, \ldots, 16\}$. Recall that she gives $A_i$ $f(i)$. We present different scenarios.

   (a) $A_1$ has 2, $A_2$ has 5, $A_3$ has 10. If they get together then can they determine the secret? If so then say how, if not then say why not. (HINT- this does NOT involve a lot of calculation.)

   (b) $A_1$ has 2, $A_2$ has 5, $A_3$ has 10, $A_4$ has 0. If they get together then can they determine the secret? If so then say how, if not then say why not. (HINT- this does NOT involve a lot of calculation.)

   (c) $A_1$ has 1, $A_2$ has 1, $A_3$ has 1, $A_4$ has 1. Has something gone wrong? Gee they all have the same number! If something has gone wrong then what is it. If not then determine the secret. (HINT- this does NOT involve a lot of calculation.)

   (d) $A_1$ has 0, $A_2$ has 0, $A_3$ has 0, $A_4$ has 0. Has something gone wrong? Gee they all have the same number! If something has gone wrong then what is it. If not then determine the secret. (HINT- this does NOT involve a lot of calculation.)

**GO TO NEXT PAGE!**

6. (30 points) Zelda has used polynomial secret sharing with $A_1, \ldots, A_9$ such that any two together can learn the secret, but one person alone cannot. She does this over mod 7. $A_1$ and$A_2$ get together! They plan to have $A_1$ reveal and then $A_2$ reveal.

   **$A_2$ is dishonest!**

   $A_1$ reveals his share and its 6. $A_2$ wants to lie and reveal a share so that $A_1$ thinks the secret is 3. Can he do this? If so then say what he reveals, and if not then show why not.