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 pseudocode for an algorithm that, on input \( N \), finds a SAFE prime between \( N \) and 2\( N \) 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 2\( N \) 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.

**SOLUTION TO PROBLEM TWO**

a) Can assume \( N \equiv 0 \pmod{30} \).
Input(\( N \))
For \( i = 1 \) to \( N/6 \)
   For \( a \in \{1, 7, 11, 13, 17, 19, 23, 29\} \)
      \( n = N + 30i + a \)
      \( m = (n - 1)/2 \)
      if TEST(\( n \))=YES then if TEST(\( m \))=YES output \( n \) and STOP.

b) We want to make sure that \( (n - 1)/2 \) is not divisible by 2,3, or 5.
If \( n - 1/2 \equiv 0 \pmod{2} \) then \( n \equiv 1 \pmod{4} \).
If \( n - 1/2 \equiv 0 \pmod{3} \) then \( n \equiv 1 \pmod{6} \).
If \( n - 1/2 \equiv 0 \pmod{5} \) then \( n \equiv 1 \pmod{10} \).
Combining this with the conditions for \( n \) not divisible by 2,3,5 we have that we must have an \( n \) such that
\[ n \not\equiv 0 \pmod{2}. \]
\[ n \not\equiv 0 \pmod{3}. \]
\[ n \not\equiv 0 \pmod{5}. \]
\[ n \not\equiv 1 \pmod{4}. \]
\[ n \not\equiv 1 \pmod{6}. \]
\[ n \not\equiv 1 \pmod{10}. \]

This is equivalent to
\[ n \equiv 3 \pmod{4} \text{ so } n \equiv 3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59 \pmod{60}. \]
\[ n \equiv 5 \pmod{6} \text{ so } n \equiv 5, 11, 17, 23, 29, 35, 41, 47, 53, 59 \pmod{60}. \]
\[ n \equiv 3, 7, 9 \pmod{10} \text{ so } n \equiv 3, 7, 9, 13, 17, 19, 23, 27, 29, 33, 37, 39, 43, 47, 49, 53, 57, 59 \pmod{60}. \]

We need the numbers that are in all three of these sets. That's just \( \{23, 47, 59\} \).

Can assume \( N \equiv 0 \pmod{6} \).

Input(\( N \))

For \( i = 1 \) to \( N/60 \)

For \( a \in \{23, 47, 59\} \)

\[ n = N + 60i + a \]

\[ m = (n - 1)/2 \]

if TEST\((n)\)=YES then if TEST\((m)\)=YES output \( n \) and STOP.

\textbf{END OF SOLUTION TO PROBLEM TWO}

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?

**SOLUTION TO PROBLEM THREE**

a) Zelda has secret \( s \).

For each \( i, 1 \leq i \leq n \), Zelda produces random \( r \) and then \( r' = r \oplus s \).

She then give \( A_i \) \( r \) and \( A_{i+1} \) \( r' \).

b)

\( A_1 \) is only involved with one pair so she gets one string.

\( A_2, \ldots, A_n \) are each involved with two pairs so they each get two strings.

\( A_{n+1} \) is involved with one pair so she gets one string.

**END OF SOLUTION TO PROBLEM THREE**

GO TO NEXT PAGE!
4. (OPTIONAL) (NOTE- the solution is based on material I did not do in class. Do not worry- this material will not be on the exam.) 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.

**SOLUTION TO PROBLEM FOUR**

Zelda generates random $r_1, r_2$ and then creates $r_3 = r_1 \oplus r_2 \oplus s$.

$A_1$ gets $r_1$

$A_2$ gets $r_2$

$A_3, \ldots, A_{10}$ secret share $r_3$ so that any three of them can find it but no two: Zelda generates random $a_2, a_1$ and looks at the polynomial

$$f(x) = a_2 x^2 + a_1 x + r_3$$

(all mod 13).

For $3 \leq i \leq 10$ she gives $A_i f(i)$.

(could also give $A_3 f(1), A_4 f(2)$, etc.

**END SOLUTION TO PROBLEM FOUR**

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.)

SOLUTION TO PROBLEM FIVE

a) NO. $A_1$, $A_2$, and $A_3$ have three points of a cubic so they cannot determine it.

b) YES. Since its a cubic and they have four points we can determine it. In fact this one is easy: since $f(1) = 1$, $f(2) = 4$, $f(3) = 9$, $f(4) = 16$. Hence $f(x) = x^2 + 1$ works. And it must BE $f(x) = x^2$ since any two cubics that agree on four points agree. The secret is the constant term which is 0. Since its over mod 17 then we think of the secret as being 0000.

5c) YES. Give then data $f(x) = 1$. So the secret is 1. No problem there.

5c) YES. Give then data $f(x) = 0$. So the secret is 0. No problem there.

(For those who thought surely something is wrong or he wouldn't have asked the question I've warned you to NOT reason that way!)

END OF SOLUTION TO PROBLEM SIX

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.

**SOLUTION TO PROBLEM SIX**

First a general thing to know: a line through $(1, a)$ and $(2, b)$ is

$$f(x) = (b - a)x + (2a - b)$$

(ADVICE- put this on your cheat sheet.)

If $A_1$ says 6 and $A_2$ says $b$ (to be determined) then they agree that $(1, 6)$ and $(2, b)$ are point on the linear function Hence

$$f(x) = (b - 6)x + (12 - b) = (b - 6)x + (5 - b)$$

$A_2$ wants $f(0) = 3$. So he wants

$$5 - b = 3$$

so $b = 2$.

**END OF SOLUTION TO PROBLEM SIX**