Week 8 Tuesday

Make sure you know your neighbor's names, and then discuss:

When generating his RSA public key, Bob secretly chooses primes p and q to generate the number $n = 253$, but then he makes an unwise decision to reveal to you that the primes p and q that he chose satisfy the equation

$$(x - p)(x - q) = x^2 - 34x + 253.$$

Use this information to find $\phi(n)$ without factoring $n = pq$.

Order, Primitive Roots, Diffie-Hellman

1. Suppose a is an integer that is not divisible by 13. Which of the following cannot be the order a mod 13?

(A) 2

(B) 3

(C) 4

(D) 5

2. What is the order of 4 mod 13?

3. Which of the following is a primitive root of 17?

(A) 2

(B) 3

(C) 4

(D) None of the above

4. Alice and Bob agree to perform a Diffie-Hellman key exchange using $p = 31$ and $g = 3$.

Alice chooses the secret integer $a = 11$. What is the integer x that she sends Bob?

5. Alice and Bob agree to perform a Diffie-Hellman key exchange using $p = 31$ and $g = 3$.

Alice chooses the secret integer $a = 11$, and receives the integer $y = 2$ from Bob. What is her shared secret with Bob?

6. Alice and Bob agree to perform a Diffie-Hellman key exchange using $p = 31$ and $g = 3$.

Eve sees Alice send Bob the integer $x = 9$ and Bob send Alice the integer $y = 27$. What is Alice and Bob's shared secret?