Week 9 Tuesday

Favorite Candy

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

Do you have a favorite candy, or did you have one when you were younger? What do (or did) you like about it? Is it something that's still around?

Elgamal

1. Bob's Elgamal public key has $p = 29$, $g = 3$, and $h = 27$.

Alice wants to send Bob the message C. She generates an ephemeral key $y = 10$. What is the ciphertext that she sends Bob?

2. Bob's Elgamal public key has $p = 29$, $g = 3$, and $h = 21$. His private key is $x = 9$.

He receives the ciphertext pair $(3, 11)$ from Alice. What was Alice's message as an integer? As a letter?

Elliptic Curves

3. Which of the following Weierstrass equations cannot be singular, no matter what real number b is chosen to be?

(A) $y^2 = x^3 + b$

(B) $y^2 = x^3 - x + b$

(C) $y^2 = x^3 + x + b$

(D) None of the above

4. Consider the elliptic curve E over the reals defined by $y^2 = x^3 + 8$. Verify that $P = (1, 3)$ and $Q = (-2, 0)$ are points on this curve, and then compute $P + Q$.

Do this in stages, and compare intermediate calculations with your neighbors as you go! Here are some *examples* of intermediate steps you could compare:

- What is the equation of the secant line through P and Q?
- What is the third point of intersection of that line with E?
- What is $P + Q$?

Make sure you're on the same page as your neighbors as you do this calculation!

5. Consider the elliptic curve E over the reals defined by $y^2 = x^3 - x + 1$. Verify that $P = (-1, 1)$ is on this curve, and then compute $2P$.

Again, do this in stages and compare intermediate calculations with your neighbors as you go!