Week 9 Wednesday

Make sure you're sitting next to someone!

Over and Over

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

If you could only choose one vacation destination for the rest of your life, where would you pick? Why?

Diffie-Hellman, Elgamal

1. 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?

2. 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?

3. 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?

4. 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?

5. 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?