JUNE 16TH CRYPTOGRAPHY PROBLEM SET

Today we are going to learn about a variant of Diffie-Hellman key exchange. ElGamal is an actual cryptosystem based on the same idea.

The idea is basically the same as Diffie-Hellman but the implementation is slightly different. Alice chooses a prime p and also g a primitive root (generator) modulo p. All computations below are done modulo p.

Alice now picks a secret number x and computes $X = g^x$ (this is Alice's paint). Alice publishes (p, g, X) (note x is hard to figure out as we discovered even using a computer). Bob would like to send a message m (a number $< p$). To do this he picks his own secret number y and computes $k = X^y = (g^x)^y = g^{xy}$ (this is the mixed paint). He also computes $Y = g^y \bmod p$ (this is Bob's paint). The encrypted message is $c = k \cdot m \bmod p$. Now Bob sends Alice the information

$$(Y, c)$$

To decrypt, Alice computes $k = g^{yx} = (g^y)^x = Y^x$, then computes the inverse d of k modulo p and finally computes

$$dc \bmod p = dkm \bmod p = (dk)m \bmod p = m.$$

ElGamal is an example of *public key cryptography.*

1. Alice chooses the prime 17 and primitive root $g = 10$. She then publishes $X = 7$. If Bob wants to send Alice the secret message $m = 2$, what would be a valid way to do that with ElGamal?

2. Now, it turns out that Alice's secret number was $x = 9$. Suppose she receives a new message $(3, 5)$. What message did Bob send to her?

3. Each group needs to choose a 2 digit prime p and a generator g (talk to me if you need help finding a generator). Choose your secret x and write your public key on board (p, g, X).

4. Prepare a message (number) to send to each other group. When all the groups are ready, go write your numbers on the board. Those groups which decrypt their received messages correctly (first) win points.

5. Now try to find the other groups secret x values. Again, points to the groups that do this quickest.