WORKSHEET #5 – MATH 5405
SPRING 2016

DUE: TUESDAY, 2/16/2016

We will play around with RSA and ElGamal. You may work in Abelian groups.

Remember, RSA works like this.

Alice chooses two big primes p, q and computes $m = p \cdot q$ and $\phi(m) = (p-1)(q-1)$. Then the group of invertible elements under multiplication mod m has size $(p-1)(q-1)$. She also chooses a number e such that

$$\gcd(e, \phi(m)) = 1.$$

Alice computes the multiplicative inverse $d \equiv e^{-1} \bmod \phi(m)$. Notice that $de = 1 + k\phi(m)$. Alice can do all this because she knows what $\phi(m)$ is.

Alice now publishes the numbers m and e. Anyone now can send a secure message to Alice. Say x is Bob's message ($x < m$). Bob compute $y = x^e \bmod m$. Alice can decrypt Bob's message by noticing that

$$y^d \bmod m = (x^e)^d \bmod m = x^{de} \bmod m = x^{1+k\phi(m)} \bmod m = x \cdot (x^{\phi(m)})^k \bmod m = x$$

Let's try it in practice.

1. Say Alice chooses the two primes $11, 17$. Then $m = 181$ and $\phi(m) = 160$. Alice also chooses the number $e = 99$. If Bob chooses to send the message made up of the number $x = 7$ to Alice, what should he send? (You may want a calculator or a phone to help do this one).

2. Now take the role of Alice, compute the number d (the multiplicative inverse of e modulo $\phi(m)$). Pretending you only know the value $y = x^e \bmod m$, compte $y^d \bmod m$ and see if you really got the x you started with.

3. You are now Eve. You notice that Alice published $m = 77$ and $e = 23$. Bob then sent the message consisting of two numbers $y_1 = 54, y_2 = 69$. Figure out what message Bob sent.

Now let's review ElGamal. 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

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

4. 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?

5. 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?