GROUP WORK – THURSDAY AFTERNOON

SPY GAMES CAMP – PSU, 2014

Computers are useless. They can only give you answers. – Pablo Picasso

1. Make a big prime n using the computer. We will use this as a modulus. Then find a generator x. Write them here and on a chalk board. Choose your own secret key a (make it big also), compute $x^a \pmod{n}$ and write it on the chalkboard too. This makes up your public key.

2. The computer can convert numbers to strings of letters and visa versa. Write a message of about 10-12 characters and convert it to a number m using the computer. Keep this number secret.

3. Find a neighboring country and identify their public key $(n', x', x'^{a'})$. Choose a b' and write for them on the chalkboard $x^{b'} \pmod{n}$ and $m \cdot x'^{a'b'} \pmod{n}$. See if they can decrypt your message.

Have them do the same for you. Note to decrypt, compute the inverse of $x^{ab} \pmod{n}$ and multiply it by the message they send you, mod n.

4. Do this with yet another country for more practice.

You have just performed ElGamal public key encryption.