

## GROUP WORK – THURSDAY MORNING

SPY GAMES CAMP – PSU, 2013

*-How long do you want these messages to remain secret? I want them to remain secret for as long as men are capable of evil. – Neal Stephenson*

We're going to learn about asymmetric ciphers. You can have complete security if you use a Vigenère cipher, with a very long random key, and never use the same key twice. But this is inconvenient. Even more, you must transmit the key securely somehow to the people you want to communicate with.

Asymmetric cryptography is about transmitting information securely over an open channel, without first communicating a secret key.

**1.** [Diffie-Hellman key exchange] Suppose Alice and Bob want to communicate over an insecure channel. Alice chooses a *BIG* prime  $p$  (this is public), and a generator  $x$  (this is also public). She then chooses a secret key  $a$  (a random number  $\leq p - 1$ ). Alice then sends to Bob the information  $p, x, x^a \pmod{p}$ . Now Bob chooses his own secret key  $b$  (a random number  $\leq p - 1$ ). He then sends  $x^b \pmod{p}$  back to Alice.

Explain why  $x^{ab} \pmod{p}$  can be computed by both Alice and Bob. This number can then be used for another cipher, say a Vigenère cipher or even a Caesar shift for instance.

**2.** How could an attacker figure out  $x^{ab} \pmod{p}$  given  $p, x, x^a$  and  $x^b$ ? (How is this related to logarithms, remember  $\log_x x^a = a$  at least in ordinary arithmetic) Do you think it is secure, for big  $p$  based on your experiments this morning?

**3.** Let's try an example, I choose a small prime  $p = 11$  and  $x = 2$  the cyclic generator. Find  $x^{ab}$  given  $x^a \pmod{11} = 6$  and  $x^b \pmod{11} = 10$ . Try it by hand and then verify it with the computer.

**4.** Choose  $p = 29$  and use the computer to help find the generator  $x$ . Choose two members of your group to be Alice and Bob. The others will be attackers (Eves). Alice computes  $x^a \pmod{p}$  and communicates this publicly and likewise Bob sends  $x^b \pmod{p}$ . Bob should send a message to Alice (say a single letter by Caesar shifted by  $x^{ab}$ ). How quickly can he decode it by hand? How long did it take the attackers to break it with a computer?

*Write down what was done.*

**5.** Now switch roles and choose a big prime  $p$  (with the help of the computer), the new Alice and Bob should use the *computer* to help send a large number  $< p$  (again by Caesar shift mod  $p$ ). See if the Eve(s) can break it within 5 minutes.