JUNE 15TH CRYPTOGRAPHY PROBLEM SET

We in science are spoiled by the success of mathematics. Mathematics is the study of problems so simple that they have good solutions.–Whitfield Diffie

As mentioned last week, there is a completely secure way to encrypt any piece of data. This is to use a Vigenére cipher with a random key as long as the message. This is totally secure as long as the key is *never used again*. Because of this, governments and businesses used to frequently have couriers with briefcases full of such keys (they still do). But this is very inconvenient for most people (you want to be able to buy something online now, not several days after you receive your key in the mail).

In the 1970s, Diffie and Hellman had a new[1] idea of how to securely communicate over an insecure channel, even if an evesdropper is listening in on everything they say.

Remember the Alice, Bob and paint example we did on the board? We need a mathematical function that has the same property. It's easy to compute, but hard to undo. Diffie and Hellman came up with modular exponentiation.

1. 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 $\leq p1$). Alice then sends to Bob the information

$$p, x, A = x^a (\bmod p).$$

Now Bob chooses his own secret key b (a random number $\leq p1$). He then sends

$$B = x^b (\bmod p)$$

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

---

[1] Or not-so-new, also see James Ellis at GCHQ.

Let's try this method (called *Diffie-Hellman key exchange*) in practice.

2. Consider the prime $p = 29$. Verify that 10 is a primitive root mod 29.

3. Alice and Bob want to find a common key to communicate securely. Alice choose the prime $p = 29$ and the primitive root $x = 10$. She choose her own secret key a and shared $15 = 10^a (\text{mod } 29)$. Suppose Bob choose his secret to be $b = 11$. Find Alice and Bobs shared key.

4. Using the same $p = 29, x = 10$, have one person in your group be Alice, another Bob, and the other three need to be Eve(sdroppers). See if Alice and Bob can find a shared key. Can the Eves find figure out what the shared key is within 2 minutes? (Have a TA or instructor time you).

5. We'll play some games with this on the board. Each team will need a prime, a generator, and a secret key.