Abstract Algebra
Lecture 23
Monday, 11/29/2010

Guest lecture by Prof. Witcher.

1 Elliptic Curve Cryptography

1.1 Cryptography

Alice and Bob. The simplest way for Alice and Bob to talk to each other is with **private key cryptography**. This sucks. If Eve wants to listen to their conversation, all she has to do is intercept the key once.

In the 70s (or earlier if you were in the British secret service) someone developed **public key cryptography**. This removes the need to send secret keys between the correspondents. This is called Diffie-Hellman key exchange (mod p). There will be two public numbers – a large prime p and a base g. Alice has her own secret integer a, and calculates $A = g^a \mod p$ and Bob has his own secret integer b and calculates $B = g^b \mod p$. Alice and Bob send each other the numbers A and B. So everyone in the world knows those two numbers. But then Alice computes $s = B^a \mod p = (g^b)^a \mod p$ and Bob computes $s = A^b \mod p = (g^a)^b \mod p$. These are the same number, the secret key that Alice and Bob will use to communicate.

If Eve wants to listen in on this conversation, she needs to know the value of s. In other words, she needs to solve the **Diffie-Hellman problem** (find g^{ab} given g^a and g^b) or she could solve the **discrete log problem** (find a givem $g^a \mod p$). The DLP can be solved in $O(e^{\sqrt{(\log p)(\log\log p)}})$. This is large, but not quite exponential. So this is actually feasible.

We seek to use this scheme, but rather than using arithemetic in $\mathbb{Z} \mod p$, we will do arithmetic in a different group. This will allow us to use not-quite-so-huge prime and still have large solving times.

1.2 Elliptic Curves

Defn: An elliptic curve $\mathcal{E}$ is the set of solutions so a Weierstrass equation

$$y^2 = x^3 + Ax + B$$

over a field $\mathbb{F}$ together with a point $\mathcal{O}$ "at infinity". We'll require $4A^3 + 27B^2 \neq 0$.

We can give $\mathcal{E}$ a group structure. To add P and Q, where P and Q are points in the elliptic curve $\mathcal{E}$, draw a line L through P and Q. L also intersects the elliptic curve R. Let R' be

the reflection of R across the x-axis. Then $R' = P \oplus Q$. There are some weird cases in this: Specifically, if P and Q are reflections of each other across the x-axis, then the line intersects the curve "at infinity", so we have $P \oplus Q = \mathcal{O}$. If we want to add $P \oplus P$, we use the tangent line of $\mathcal{E}$ at P for the line L. Note that $R \oplus \mathcal{O} = R$, since the third intersection is at R', and then we reflect that point, which gives us back R.

Theorem: $\mathcal{E}(\mathbb{C})$ is an abelian group under $\mathcal{O}$.

Proof: We know the identity is $\mathcal{O}$. Commutativity is pretty easy, since it doesn't matter what order we look at points on a line. Associativity is much harder, but can be shown. ■

Our addition formula, so we don't have to draw lines with our ruler, is:

$$P_1 = (x_1, y_1), \qquad P_2 = (x_2, y_2), \qquad P_2 \neq P_1'$$

$$P_1 \oplus P_2 = (x_3, y_3)$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

Note that none of this seems particularly dependent on the real numbers. So lets work over some finite field $\mathbb{F}_p$ instead. Let $p \geq 3$, and let

$$\mathcal{E}(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + Ax + B\} \cup \{0\}$$

Theorem: Let $P, Q \in \mathcal{E}(\mathbb{F}_p)$.

- $P \oplus Q \in \mathcal{E}(\mathbb{F}_p)$.
- $\mathcal{E}(\mathbb{F}_p)$ is a finite abelian group under $\oplus$.

1.3 ECC

So now lets do Diffie-Hellman key exchange using our elliptic curves. We'll need a large prime p, an elliptic curve $\mathcal{E}(\mathbb{F}_p)$, and a point $P \in \mathcal{E}(\mathbb{F}_p)$. The secret parameters are: Alice chooses a, and then calculates $Q_A = P \oplus \cdots \oplus P = aP$, and Bob chooses b and calculates $Q_B = bP$. They exchange Q_A and Q_B. They each compute bQ_A and aQ_B, which gives them the same, secret, point $S = abP$ on the elliptic curve.

So what does Eve need to do to break this? She can solve:

- the Elliptic curve discrete log problem (find a given P and aP).
- the Diffie-Hellman problem for elliptic curves (find abP given aP and bP).