Math 4400
Week 14, Thursday
Elliptic curve cryptography.

Recall: The Diffie-Hellman key exchange.

Public: p a large prime, g a primitive root mod p.
$(g \in \mathbb{F}_p^\times)$

Private: Alice picks integer a, Bob picks integer b

Public: Alice transmits $\alpha = g^a$, Bob transmits $\beta = g^b$

Private: Alice computes β^a, Bob computes α^b

Shared secret: $s = \beta^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = \alpha^b$

Depends on difficulty of discrete log in $\mathbb{F}_p^\times$.
Given g and g^x, no efficient way to compute x

Idea of elliptic curve cryptography — can replace $\mathbb{F}_p^\times$ with any group where it is easy to compute large multiples (powers) but hard to find n given g and ng

Elliptic curves over finite fields:
Suppose $\mathbb{F}$ is a finite field of characteristic >3 (e.g. $\mathbb{F}_5$) and $x^3 + Ax + B \in \mathbb{F}[x]$ does not have a repeated root.

Then: The solutions to $E: y^2 = x^3 + Ax + B$ in $\mathbb{F}^2$ + an extra point ∞ form a commutative group $E(\mathbb{F})$ using addition formulas like we derived in class on Tuesday.

Elliptic curve cryptography:

Public: The equation for the elliptic curve E and $P \in E(\mathbb{F})$

Private: Alice picks integer a, Bob picks integer b

Public: Alice transmits $\alpha = aP = \underbrace{P+P+\cdots+P}_{a \text{ times}}$, Bob transmits $\beta = bP$

Private: Alice computes $a\beta$, Bob computes $b\alpha$

Shared secret: $s = a\beta = a(bP) = b(aP) = b\alpha$

s is an element of $E(\mathbb{F})$ i.e. $(x,y) \in \mathbb{F}^2$ s.t. $y^2 = x^3 + Ax + B$.

Depends on difficulty of discrete log in $E(\mathbb{F})$

Given P and xP, no efficient way to compute x.

In class on Thursday we'll carry out a key exchange.

Why ECC? Takes fewer bits to make decryption hard!
(I.e. this discrete log problem is harder)