Elliptic Curve Diffie-Hellman Key Exchange

Trusted Party

- Generate $E(\mathbb{F}_p) : Y^2 = X^3 + AX + B$ and $P \in E(\mathbb{F}_p)$ of large prime order q
- Publish (p, A, B, P, q)

Alice

- Select n_A where $1 < n_A < q$
- Compute $Q_A = n_A P \in E(\mathbb{F}_p)$
- Send Q_A to Bob

Bob

- Select n_B where $1 < n_B < q$
- Compute $Q_B = n_B P \in E(\mathbb{F}_p)$
- Send Q_B to Alice

Shared key is $Q = n_A n_B P = n_B n_A P$

The Trusted Party Store publishes toy credentials

$(p, A, B, P, q) = (953, 13, 12, (375, 647), 113)$

1. Verify that P lies on the elliptic curve.
2. Use `http://www.christelbach.com/eccalculator.aspx` to verify that $\text{ord}(P) = q$
3. You and Bob are implementing ECDHKE by sharing only x-components.
   (a) If you pick $n_A = 102$, what is the value you send to Bob?
   (b) If you receive 362 from Bob, what is your shared key?