# To what extent can elliptic curves be used to establish a shared secret over an insecure channel?

### Outline

1. Describe $\mathbb{Z}_p^\times$ as a group
   a. Group properties: closure, invertibility, existence of identity, associativity
2. Describe the discrete log problem
   a. Go over an example
3. Describe how the discrete log problem is used for diffie-hellman key exchange
4. A sketch/example on index calculus with finite field diffie-hellman
   a. Then explain general number field sieve and how that as a special form of index calculus can speed things up.
5. Describe how elliptic curves form a group
   a. Then, how elliptic curves can also be used for diffie-hellman key exchange.
6. Formalize pollard's $\rho$ algorithm, and how it can attack discrete logs for groups in general, in $O(\sqrt{n})$ time.
7. Comparison for space efficiency for elliptic curves, size of group elements for elliptic curves compared to finite fields.

### Tentative Table of Contents