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

1. Describe $\mathbb{Z}_p^\times$ as a group
2. Describe the discrete log problem
3. Describe how the discrete log problem is used for diffie-hellman key exchange
4. Describe how elliptic curves form a group
5. Attacks on discrete logs in general groups (elliptic curves): pollard's ρ algorithm
6. Attacks on discrete logs in $\mathbb{Z}_p^\times$: index calculus and the general number field sieve
7. Comparison for space efficiency for elliptic curves, size of group elements for elliptic curves compared to finite fields.