- Introduction: talk about uses of ECDH, having a shared secret
- Introduction II: What are elliptic curves? Working with Wierstrauss forms. The group law for elliptic curves, projective geometry, proof of some properties. Question: do we needd to explain group theory?
- Discrete log problem in groups, how the index calculus defeats the multiplicative groups modulo a prime for small primes. https://security.stackexchange.com/questions/112313/what-is-the-current-security-status-of-diffie-hellman-key-exchange as a start, but find better sources than that.
- Discrete log problem in an elliptic curve
- Detailed step by step description of ECDH:
  - Randomly pick a point, how do we do that? (Mathematical, not computer science) Share that point to others
  - Add that point to itself n many times on Alice, sends g^n to bob, m many times on Bob, sends g^m to Alice. Alice computes g^{mn} and bob computes g^{nm}. (from wikipedia)
  - What specific powers of integers do we select?
  - Hashing that shared secret to be used as a shared secret for https.
- Useful for establishing secure connection to online banking, hide the contents that you see from your internet service provider, provides privacy.
- Elliptic curve is also more secure - ref https://en.wikipedia.org/wiki/Logjam_(computer_security) Logjam
  - logjam talks about imperfect forward secrecy
  - https://crypto.stackexchange.com/questions/70464/what-is-the-actual-result-of-a-logjams-dh-attack
- https://crypto.stackexchange.com/questions/52618/why-do-elliptic-curves-require-fewer-bits-for-the-same-security-level
- Some notes
  - Should have balance between text, math, and visuals
  - A good strategy is to use some examples
- https://en.wikipedia.org/wiki/Security_level