Exercise 1: Certificate Check

In class we said that failing to check the sender of a certificate allows for a man-in-the-middle attack. Go through the actual steps and messages that would be sent to accomplish it.

Exercise 2: Certificate Revocation

In class we discussed a number of different certificate revocation strategies: CRL, CRL deltas, short-lived certs, OCSP, and OCSP stapling. Compare them in terms of communication cost and security cost (e.g., time of breach to time of revocation).

Exercise 3: TLS Defenses

In class we discussed the design of TLS. For each of the following threats and attacks, what aspect of TLS is designed to protect against it?

- replay attacks
- reflection attacks
- TLS version downgrade attack
- ciphersuite downgrade attack
- eavesdropping
- message deletion
- message modification
- man-in-the-middle attack
- impersonation attack