Course Intro

SSL/TLS: 2 parts

1. handshake: to establish a shared secret key
2. record layer: actual communications with shared key

Encrypted Files

- on disk, 2 guarantees

1. **confidentiality**
2. **integrity**

Symmetric Encryption

- shared secret key
- (E, D): cipher, where E is encryption, D is decryption
- m is the *message*, c is the *ciphertext*, k is the *key*
- $E(m, k) = c$, $D(c, k) = m$
- E,D are public knowledge. k is the only secret (other than m, obviously

Use Cases

- single-use keys: new key for every message
- multi-use keys: 1 keys, many messages.
  - needs "more machinery"

What Is Cryptography?

Capabilities

- message integrity
- secured communication
- digital communications ("mix nets" a la Tor)
- anonymous digital cash

Protocols

- elections: keep notes secret but winner verified
  - can't reveal individual votes, but "election center" and voters know and verify the winner

- private auction: “vickery auction” whereby thighest bidder wins, but pays 2n dhighest prices.
  - actual highest bid should be secret
  - only reveal 2nd highest bid and winner’s identity
  -