Advanced Cryptography and PKI

- *crypto service provider* - calls crypto functions as a service
- *digital certificate* - associates a user's *identity* with their public key
- *master secret* - used to derive session keys
- A *Cipher Suite* is the combination of encryption, signing, and hashing algorithms supported

Three characteristics of *key strength*:

- randomness
- length
- cryptoperiod - expiration

  Need to explore about half of keyspace in order to break

Block Cipher Modes of Operation:

- Electronic Code Block (ECB)
  - Each plaintext block is ciphered separately - orthogonal map
- Cipher Block Chaining (CBC)
  - Block is ciphered, ciphertext is XORd with next plaintext block
- Counter (CTR)
- Galios / Counter (GCM)
  - Encrypts the plaintext and includes an encrypted MAC

PKI

- *Certificate Authorities* issue digital certificates
  - They may be arranged *heirarchical* (one master / root, self-signed CA)
  - *distributed* (tree of CAs)
  - *bridge* - link between multiple CA networks, with one acting as a *facilitator*
- *Certificate Repositories* manage a centralized directory of digital certificates
- *Certificate Revocation Lists* declare what certificates are no longer (or temporarily) invalid
- *Online Certificate Status Protocol* (OCSP) checks a cert's status
- *Extended Validation Certificates* showcase the name of the company, as further trust. FIXME
- *Certificate Policies* are a set of rules that govern the operation of PKI
- *Certificate Signing Request* (CSR) - how someone associates their identity to their public key
- *Subject Alternative Name* (SAN) / *Unified Communications Certificate* (UCC) - an extension to a certificate to include one or more domain names, or a user principal name (UPN), for added identity authenticity.
- *Web-Client Certificates* ensure for a web-browser that a web-server is authentic w.r.t. their domain.

- *Certificate Practice Statement* (CPS) is a document detailing how a CA manages its certificates, and how to register for one
- *Domain Validation Digital Certificate* - validates control over the domain name
- *Extended Validation* - Allows enhancing the certificate with the company name for further validation
- *destruction* - removing affiliation with a certificate, and private / public keys

Four stages of certificate life cycle:

- Creation
- Suspension
- Revocation
- Expiration

  Distributed trust is the basis for most trust models on the internet, but there exists others as well, including 3rd-party trust models.

- A distributed CA model, where only one CA facilitates all other CAs is considered a 3rd party trust model.

IPSec

- Authentication Header - Integrity
- Encapsulating Security Payload - Confidentiality
- *transparent* - nobody has to install anything to use it
- useful for VPNs
- manages Authentication, Confidentiality, and Key-Management