Encryption and Security in Transit

- Attacker Posture
    - Inside/outside
        - Firewall
        - Broadcast domain / subnet
    - Man-in-the-middle (MITM)
- Crypto
    - Symmetric key cryptography
    - Key management
        - Shared key
        - Pairwise key
    - Asymmetric key cryptography
        - Asymmetric key agreement (DH example)
        - Asymmetric signature (RSA example)
        - Trust / PKI
            - Certificate Authorities
            - CA Root Chain
            - Obtaining a Certificate (Let's Encrypt)
            - Certificate Transparency
    - Protocols
        - SSL/TLS
            - https://www.ssllabs.com
            - HTTPS vs SMTP
            - SNI
        - SSH
        - IPsec
            - Encrypted tunnels
    - Details
        - Encryption, Authentication, Integrity, Privacy
        - Cipher modes
        - End-to-end vs hop-by-hop
        - Proxies and off-loading