How does email work?
- fills out a header: To, From, Subject …
- RFC 822: how Mail initially worked, basic set of fields necessary (not much)
  - incredibly easy to spoof (ASCII Coded)
- MIME: multipurpose internet mail extension
  - standard, importantly introduced attachments
  - convert binary file to base 64 encoding to be able to send over mail system
- S/MIME: set of enhancements to mime (secure)
  - 4 new functionalities:
    - enveloped data
    - signed data: need S/MIME based interface
    - clear signed data: don’t need S/MIME based interface
    - signed and enveloped
  - creates a digest encoded with public key of recipient
  - Mapped using radix 64 encoding
  - Enveloped data - 3DES
    - clients must understand SMIME protocols
- Domain Key Identified Mail (DKIM)
  - move responsibility from user back to administrative domain level
  - Authenticated @ administrative domain
    - 1 domain can query another domain to get that info
    - admin domain guarantees message was sent by them
- Components:
  - MUA - Message User Agent: responsible for interfacing with w/ user
  - Message Transfer system (responsible for hop-hop)
    - like a router, move message from user to dest.
- Strategy behind DKIM
  - both sides must participate
  - …
  - In DKIM signature covers content & some of the header
    - can’t have spoofed origination

SSL: secure socket layer
TLS: transport layer security
  - basic concept: encrypt when sending, decrypt when receive
  - 2 part protocol:
    - bottom: record protocol
      - responsible for large amount of work
      - need something that initiates connection (session)
      - Handshake: decide on encryption and hashing
    - upper: any # of higher level protocols
      - 3 req.: handshake, alert, cipher spec (“go”)
        - alert = “warning or failure”
-Other: EX: http: talking to SSL Record Layer
  -P@P relationship b/tw 2 SSL/TLS layers
-Record level: 2 services
  -confidentiality: shared secret key
  -integrity: also defines key used for hash algorithms
-SSL can happen @ application or session level