Mail: builds set of headers

- Easily spoofed headers originally (ASCII) (RFC 822)

- MIME standards defined attachments
  
  o Encoding (base 64): takes file, encodes binary to ASCII that can be sent

- S/MIME – secure mime (allows secure attachments)
  
  o 4 new functions to MIME

    1) Enveloped data

    2) Signed data

    3) Clear signed data

    4) Signed & enveloped data

- Signed & clear signed data:
  
  o Digital signature & SHA-1

    o Mapped using radix64/base64 encoding

- Enveloped Data (El Gamal)

  o Private/public key

  o Session key with triple DES

    ▪ Transmitted using certificates

- Problems: requires clients to understand S/MIME

- DKIM: takes responsibility from the client, moves to domain admin (like ISP)

  o Has authenticated, active domain level

  o Allows query to happen automatically (at domain level)

- Consists of MUA, MDS, MSA, MTA to transfer and receive messages
SSL: secure socket layer (aka TLS):

- TLS: transport layer security, one of most widely used services

- 2 layer protocol:
  1) Record protocol/layer: does a lot of the work
  2) Higher level protocols: handshake, alert, change cipher spec, heartbeat and HTTP sit on top, talk to record layer

  o Peer to peer connection between TLS layers

- Can make ssl part of protocol suite, or embed in specific packages

- 2 TLS concepts:
  o TLS Session
  o TLS Connection

- Change cipher spec: simplest protocol, sole purpose is to cause pending state (single byte) to be copied to current state.

- Alert protocol: error/warning messages, may terminate connection

- Handshake protocol: most complex, done before data transferred

  o Clients must authenticate each other, negotiate encryption algorithm, then exchange keys