Secure Email

• Requirements:
  – Secrecy
  – Sender, receiver authentication
  – Message integrity

• Secrecy
  – Can use public keys to encrypt messages
    • Inefficient for long messages
  – Use symmetric keys
    • Alice generates a symmetric key K
    • Encrypt message M with K
    • Encrypt K with EB
    • Send K(M), EB(K)
    • Bob decrypts using his private key, gets K, decrypts K(M)

Secure Email

• Authentication and Integrity (with no secrecy)
  – Alice applies hash function H to M (H can be MD5)
  – Creates a digital signature DA(H(M))
  – Send M, DA(H(M)) to Bob

• Putting it all together
  – Compute DA(H(M))
  – M' = { M, DA(H(M)) }
  – Generate symmetric key K, compute K(M')
  – Encrypt K as EB(K)
  – Send K(M'), EB(K)

• Used in PGP (Pretty Good Privacy)
Secure Sockets Layer (SSL)

- SSL enhances TCP with security services
  - Server authentication, confidentiality, data integrity, client authentication (optional)
- SSL can be employed by any application that runs over TCP.
  - e.g., between Web browsers and servers for e-commerce (https)

SSL mutual authentication.
Example: Kerberos

Authentication in Kerberos

Setting up a secure channel in Kerberos