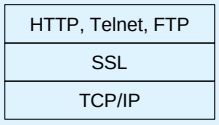
Anwendungen in Computernetzen
WS 2000/2001

Probleme im Internet
Sicherheit

- Firewalls:
  Ein Firewall in einem lokalen Netz dient dazu, den unautorisierten Zugriff von außerhalb zu verhindern.

Probleme im Internet
Sicherheit

- Secure Sockets Layer (SSL):
  Das SSL Protokoll soll sichere Kommunikation am Internet ermöglichen.



Probleme im Internet
Sicherheit

- Technik des SSL:
  - Public Key Verfahren
  - RSA-Verschlüsselung
  - http://dir.yahoo.com/Computers_and_Internet/Internet/World_Wide_Web/Security_and_Encryption/Secure_Sockets_Layer__SSL__Protocol

Probleme im Internet
Sicherheit

- Eigenschaften des SSL:
  - Server-Authentifizierung
  - Verschlüsselung von Daten
  - Integrität transferierter Daten
- Einsatzgebiete:
  - Electronic Cash
  - Electronic Banking

Probleme im Internet
Sicherheit

- Pretty Good Privacy (PGP):
  PGP ist ein System zur Authentifizierung von E-Mails.
  - Verschlüsselung: Public key des Empfängers
  - Authentifizierung: Mails werden mittels secret key des Senders mit einer Signatur versehen. Der Empfänger kann die Signatur mit dem public key des Senders nachprüfen.

Probleme im Internet
Sicherheit

- Rechtslage bei PGP:
  - PGP ist in den meisten Ländern legal verwendbar.
  - PGP darf allerdings nicht aus den USA exportiert werden (Auch nicht in angewandter Form).
  - Digitale Unterschrift mit PGP:
    Genauso wie mit herkömmlichen Dokumenten.