Netzwerke – Seminaristische Übung WS17/18

Application Layer

Benjamin.Troester@HTW-Berlin.de
PGP: ADE1 3997 3D5D B25D 3F8F 0A51 A03A 3A24 978D D673

Benjamin Tröster

5. Januar 2018

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Road-Map

1. Orga
2. Retrospektive
3. Application Layer
   - SSH
   - Crypto

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Nerd-Wochenmarkt

Empfehlung der Woche:

- Chaos Communication Congress – 34c3
  - NIC: `https://media.ccc.de/v/34c3-9159-demystifying_network_cards`
  - Hacker Jeopardy: `https://media.ccc.de/v/34c3-9007-hacker_jeopardy`
- Media CCC
  - `https://media.ccc.de/c/34c3`

- Das Semester ist (fast) vorbei!
- D.h. das Testat steht an...
  - 1. Gruppe – 19.01.2018, $15^{\underline{45}} - 19^{\underline{00}}$ Uhr
  - 2. Gruppe – 15.01.2018, $8^{\underline{00}} - 12^{\underline{00}}$ Uhr
  - Gruppe zu maximal vier Studierenden
  - Seien Sie bitte pünktlich!
- Zur Klausurvorbereitung werden diese Woche Übungsblätter Online gestellt (Mail an mich, wenn es Freitag nach 21 Uhr noch nicht online ist!)
- Rechnen Sie ausreichend Zeit für die Vorbereitung auf Klausuren etc. ein!
- Für die Übungsblätter – ~1-2 Stunden (bei gutem Vorwissen), ohne 3-4 Stunden
- Bedarf an weiteren Aufgaben?

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

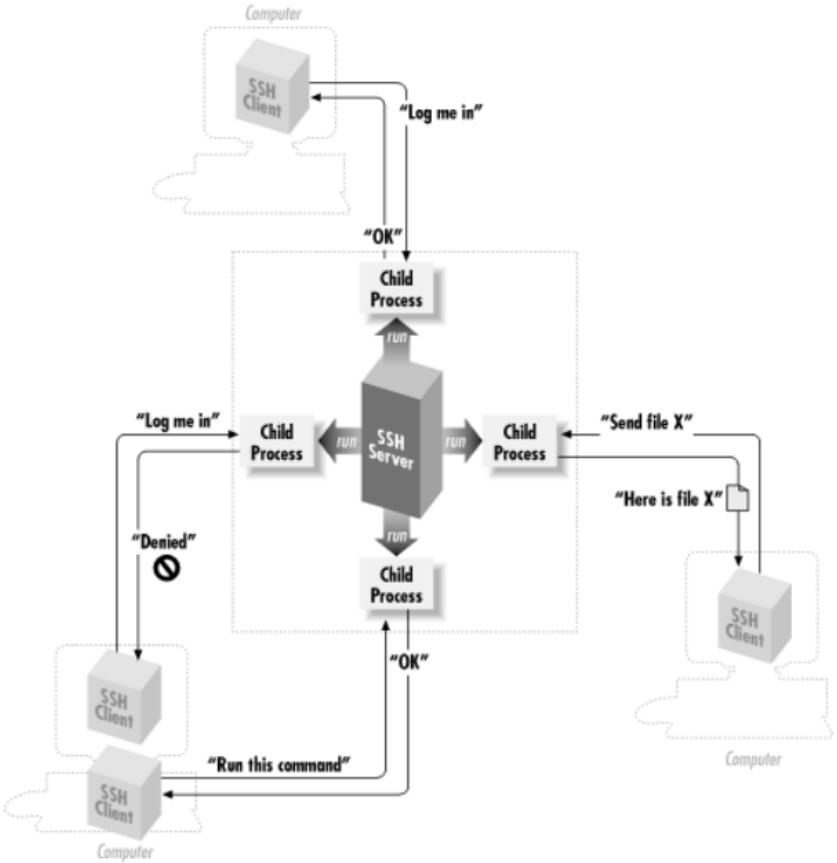
Retrospektive

- Vorlesung
  - Wo stehen Sie in den Vorlesung?
  - Fragen?
- Übungsblatt 4 & 5 – Routing
  - Stand der Gruppen
  - Fragen?

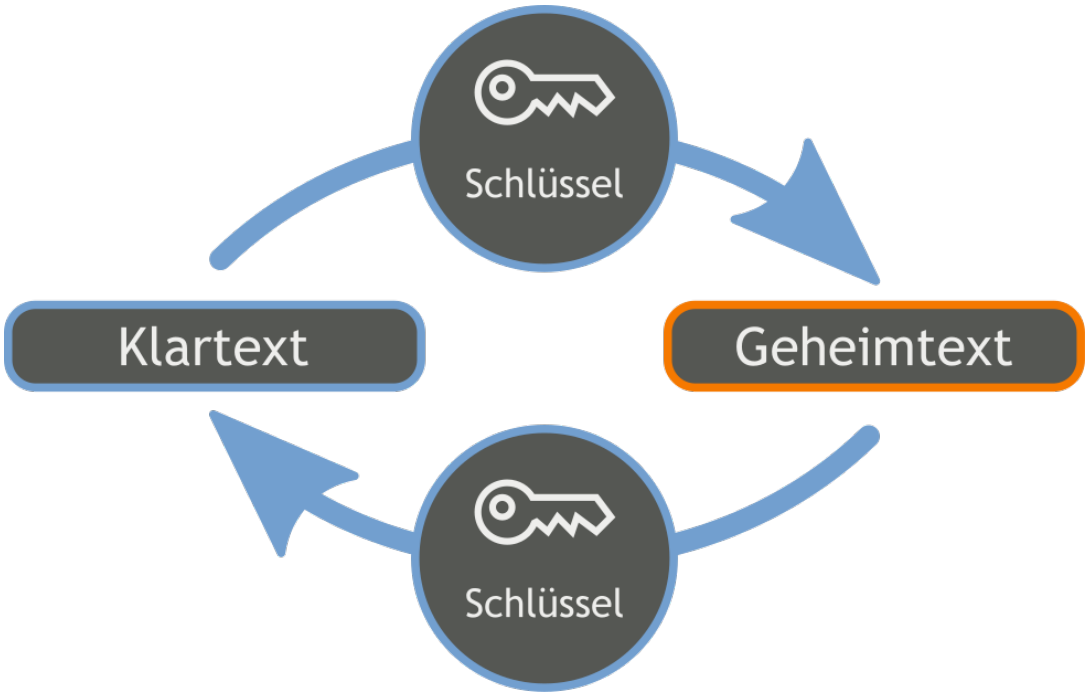

OpenSSH
SSH...

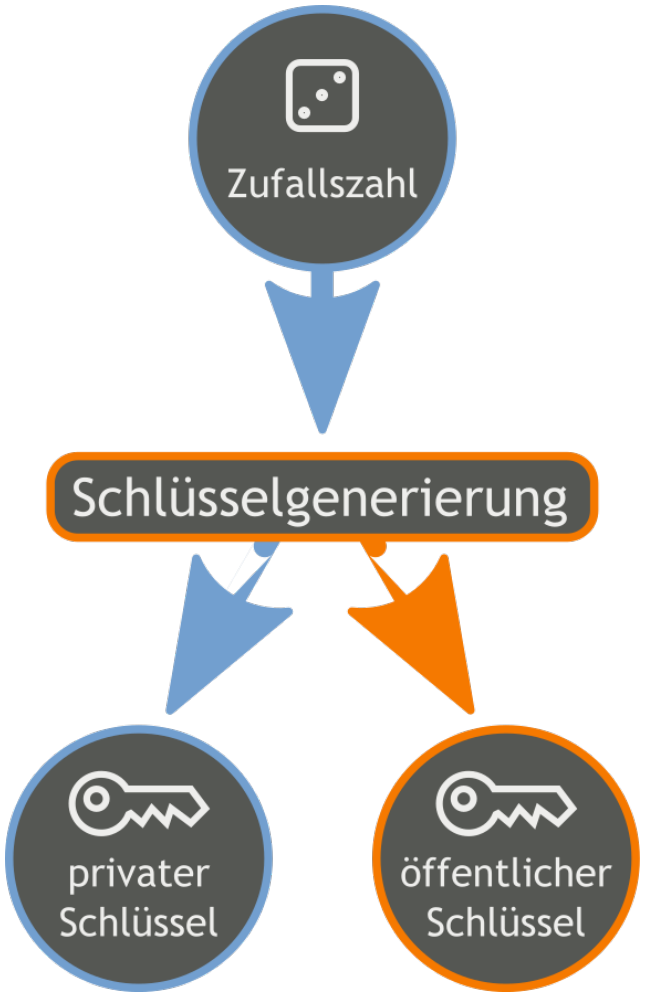
SSH

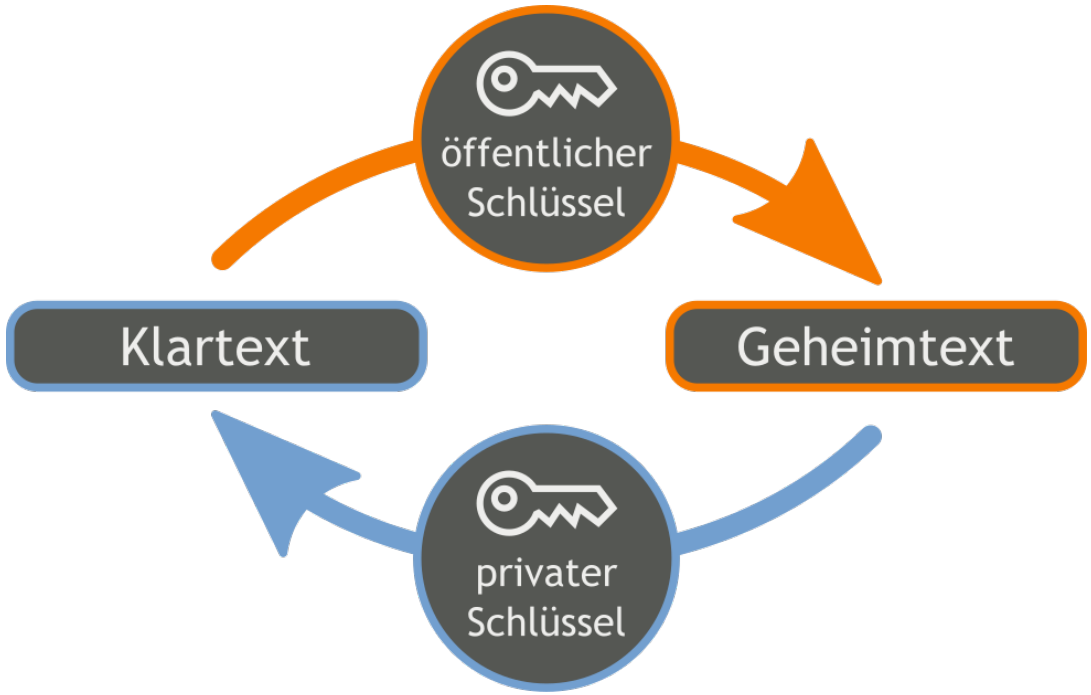
- SSH – Secure Shell
- Sammlung von Programmen/Diensten & Protokolle zur sichere Netzwerkkommunikation
- Sicherung der Kommunikation durch:
  - Kryptografie
- Aufgaben:
  - Verschlüsselung der Daten
  - Integrität von Daten
  - Authentizität des Absenders
  - Autorisierung – nur Befugte könne die Daten einsehen

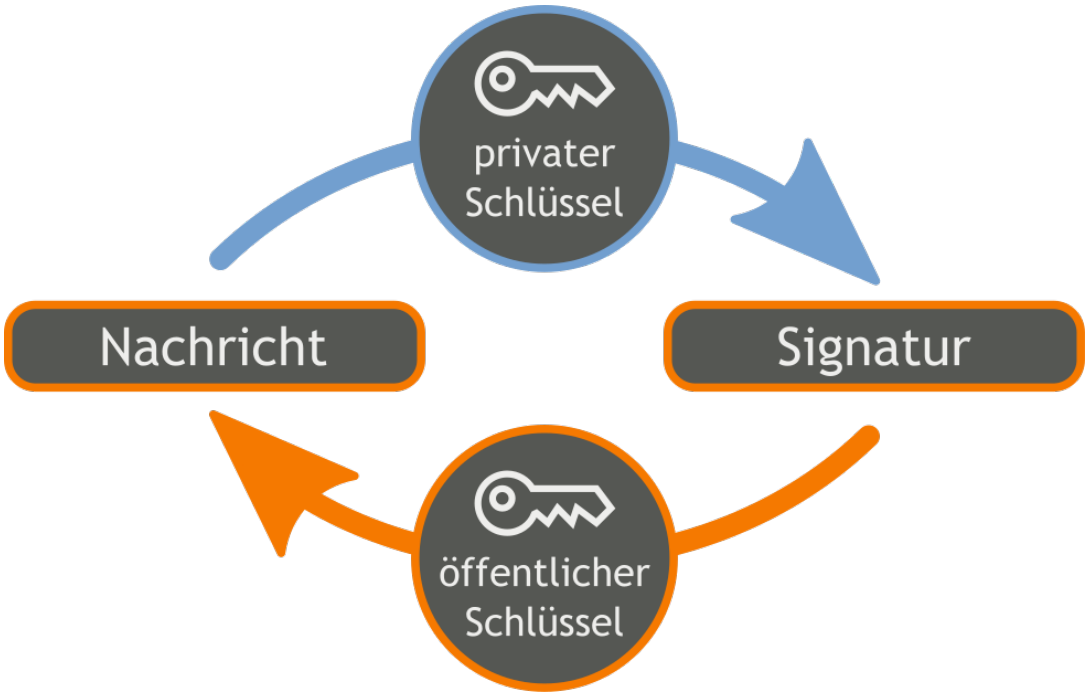

Computer
SSH Client
"Log me in"
"OK"
Child Process
run
"Log me in"
Child Process
run
SSH Server
run
Child Process
"Send file X"
"Here is file X"
"Denied"
Child Process
SSH Client
"OK"
SSH Client
"Run this command"
SSH Client
Computer
Computer

- Arten von Chiffren:
  - Symmetrische Chiffren
    - AES, Towfisch, 3DES, RC2, RC4, RC5, RC6, One-Time-Pad, Serpent, ...
    - Unterscheidung in Stromchiffre und Blockchiffre
    - Verschiedene Verfahren haben unterschiedliche Modi – CBC, EBC etc.
  - Asymmetrische Chiffren
  - RSA, Merkle-Hellman, Diffie-Hellman, Elgamal, ...
  - Generierung eines Schlüsselpaars – private & public
  - Funktionsweise aufgrund von mathematisch schwer lösbaren Problemen
  - Faktorisierungsproblem, diskretes Wurzelziehen (e-te Wurzel mod N), diskreter Logarithmus, ...


Schlüssel
Klartext
Geheimtext
Schlüssel


Zufallszahl
Schlüsselgenerierung
privater Schlüssel
öffentlicher Schlüssel


öffentlicher Schlüssel
Klartext
Geheimtext
privater Schlüssel


privater
Schlüssel
Nachricht
Signatur
öffentlicher
Schlüssel