Netzwerke – Übung WiSe2018/19

IT Security

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

Benjamin Tröster

Road-Map

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

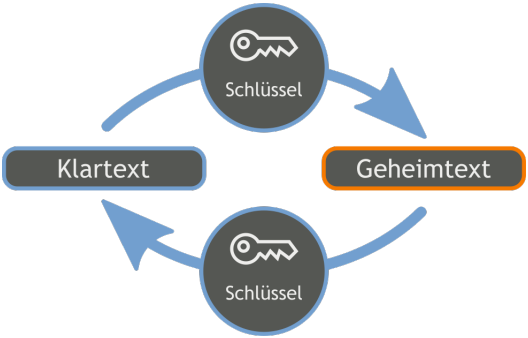
- Crypto
- SSH

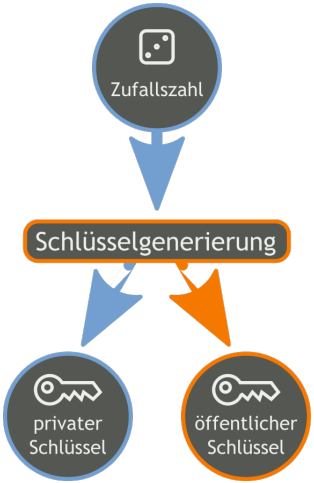
Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

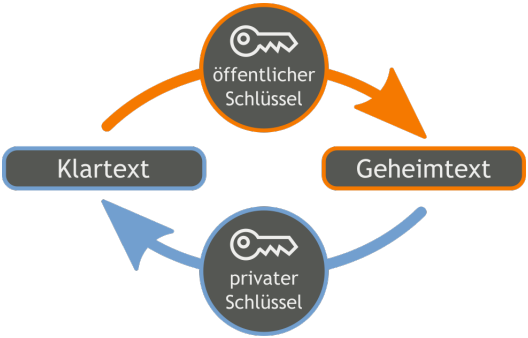
Aktueller Stand

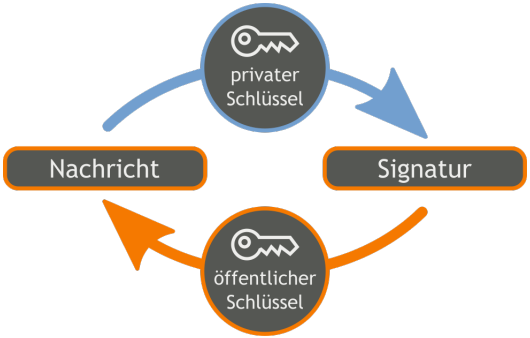
- Anwendungsprotokolle und Analyse des Netzwerkverkehrs
- Einige ausgewählte Protokolle:
  - DNS
  - HTTP(S)
  - IMAP, SMTP
- Erste Berührungspunkte mit Crypto – *openssl*

- 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: Einwegfunktionen
  - Faktorisierungsproblem, diskretes Exponentiation/Wurzelziehen ($\sqrt[\alpha]{n} \mod N$), diskreter Logarithmus, ...


Schlüssel
Klartext
Geheimtext
Schlüssel


Zufallszahl
Schlüsselgenerierung
privater Schlüssel
öffentlicher Schlüssel


öffentlicher Schlüssel
Klartext
Geheimtext
privater Schlüssel

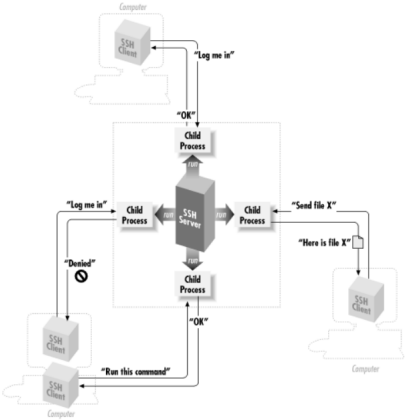

privater
Schlüssel
Nachricht
Signatur
öffentlicher
Schlüssel


OpenSSH
SSH...

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

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