

Netzwerke – Übung SoSe 2019

IT Security

Benjamin.Troester@HTW-Berlin.de

PGP: ADE1 3997 3D5D B25D 3F8F 0A51 A03A 3A24 978D D673

Benjamin Tröster

Road-Map

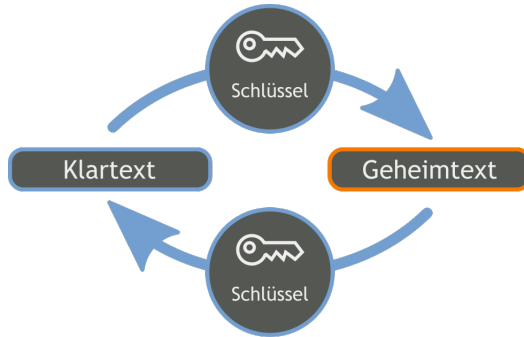
- 1 Aktueller Stand
- 2 Kryptografie

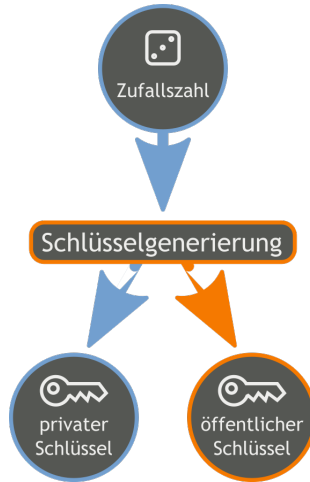
- Crypto
- SSH

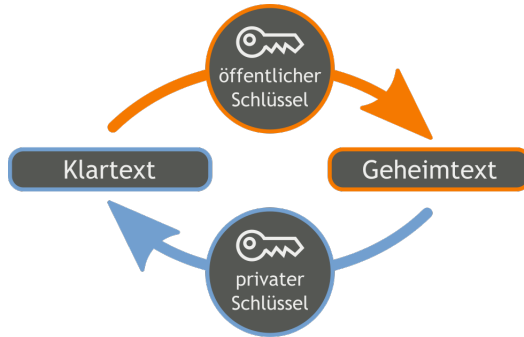
Aktueller Stand

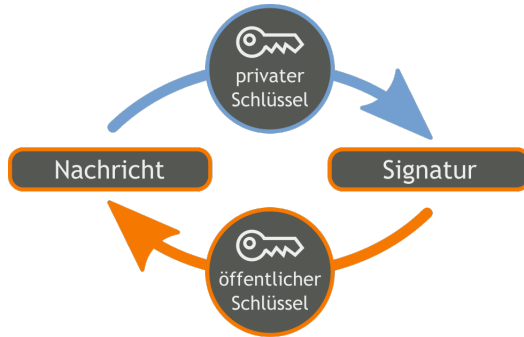
- Anwendungsprotokolle und Analyse des Netzwerkverkehrs
- Einige ausgewählte Protokolle:
 - DNS
 - HTTP(S)
 - IMAP, SMTP
- Erste Berührungspunkte mit Crypto – *openssl*

- 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 ($\sqrt[\alpha]{n} \bmod N$),
diskreter Logarithmus, ...











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

