

openHPI-Kurs: Wie funktioniert das Internet?
Sicherheit im Internet?

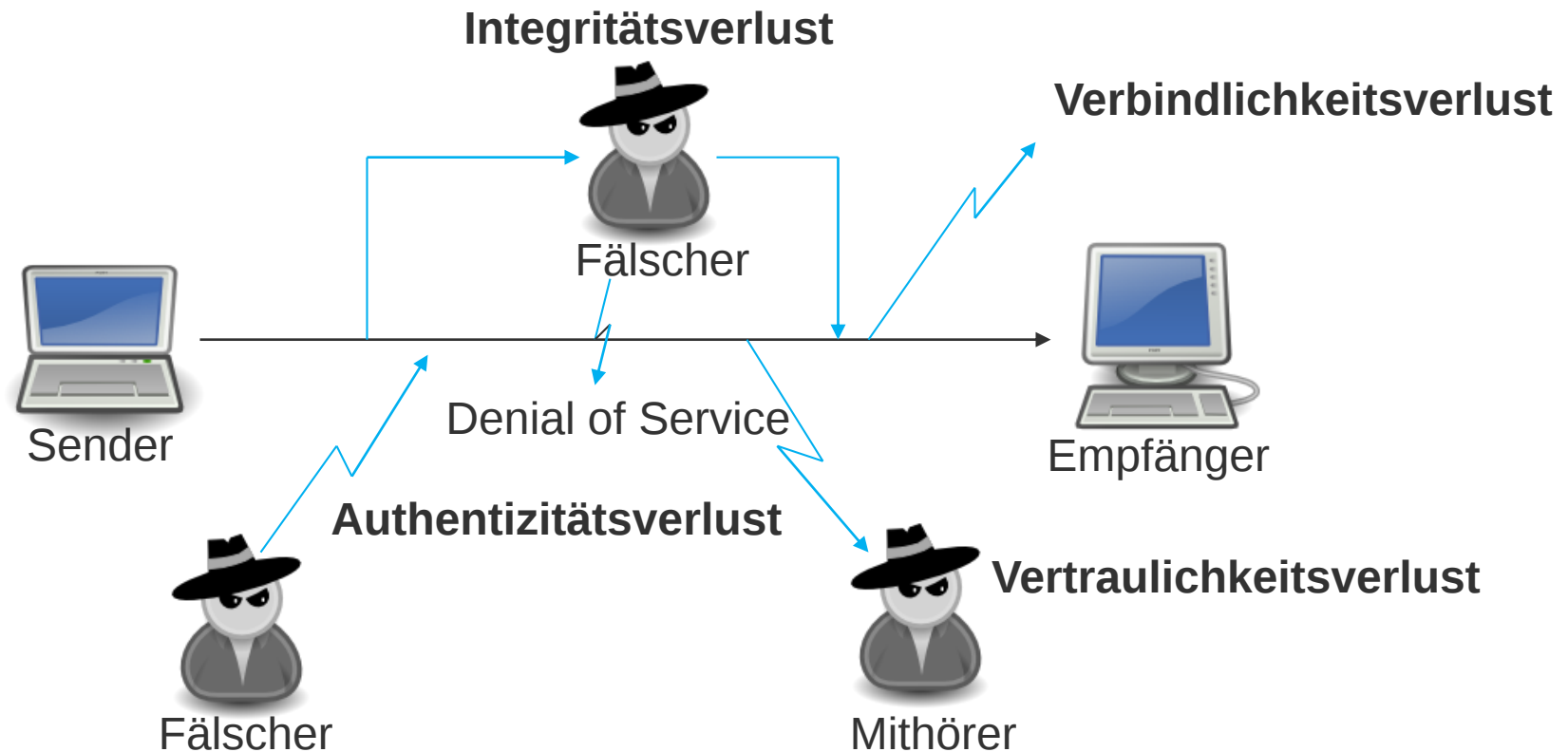
Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut
Universität Potsdam

Sicherheit im Internet (1/7)

Verschiedene Aspekte der Sicherheit spielen wesentliche bzw. entscheidende Rolle für die Nutzung von Rechnernetzen

- **Geschlossene Netze** bilden eigenständige Inselnetzwerke, auf die von außen ohne physikalischen Zugang nicht zugegriffen werden kann
- **Offene Netze** verfügen über Anschluss an weltweites Internet und bieten so Zugriff von außerhalb
 - Offene Netze sind einer Vielzahl von Bedrohungen ausgesetzt

Unterschiedliche Arten der Bedrohung in Kommunikationsnetzen und im Internet:



Sicherheit im Internet (3/7)

Analyse der Bedrohungsarten führt zur Formulierung von **Sicherheitszielen**:

- **Vertraulichkeit / Privacy**

- ☐ Bedrohung z.B. durch Abhören („Eavesdropping“)

- **Authentizität / Authenticity**

- ☐ Bedrohung z.B. durch Vortäuschung eines falschen Absenders („Spoofing“)

- **Integrität / Integrity**

- ☐ Bedrohung z.B. durch Datenverfälschung bei Übertragung

- **Verbindlichkeit / Non-Repudiation**

- ☐ nicht abstreitbare, rechtsverbindliche Datenübertragung

- **Verfügbarkeit / Availability**

- ☐ Bedrohung z.B. durch gezielte Überlastung („Denial of Service“)

Sicherheit im Internet (4/7)

Man unterscheidet

- **aktive Angriffe**

- Angreifer verfälscht Inhalte, manipuliert Authentizität, überbeansprucht Netzdienste, usw.

- **passive Angriffe**

- Angreifer hört Kommunikation ab, spioniert Netzwerk aus, zeichnet Kommunikation auf, ...

Aktive Angriffe sind leichter zu erkennen als passive...

Sicherheit im Internet (5/7)

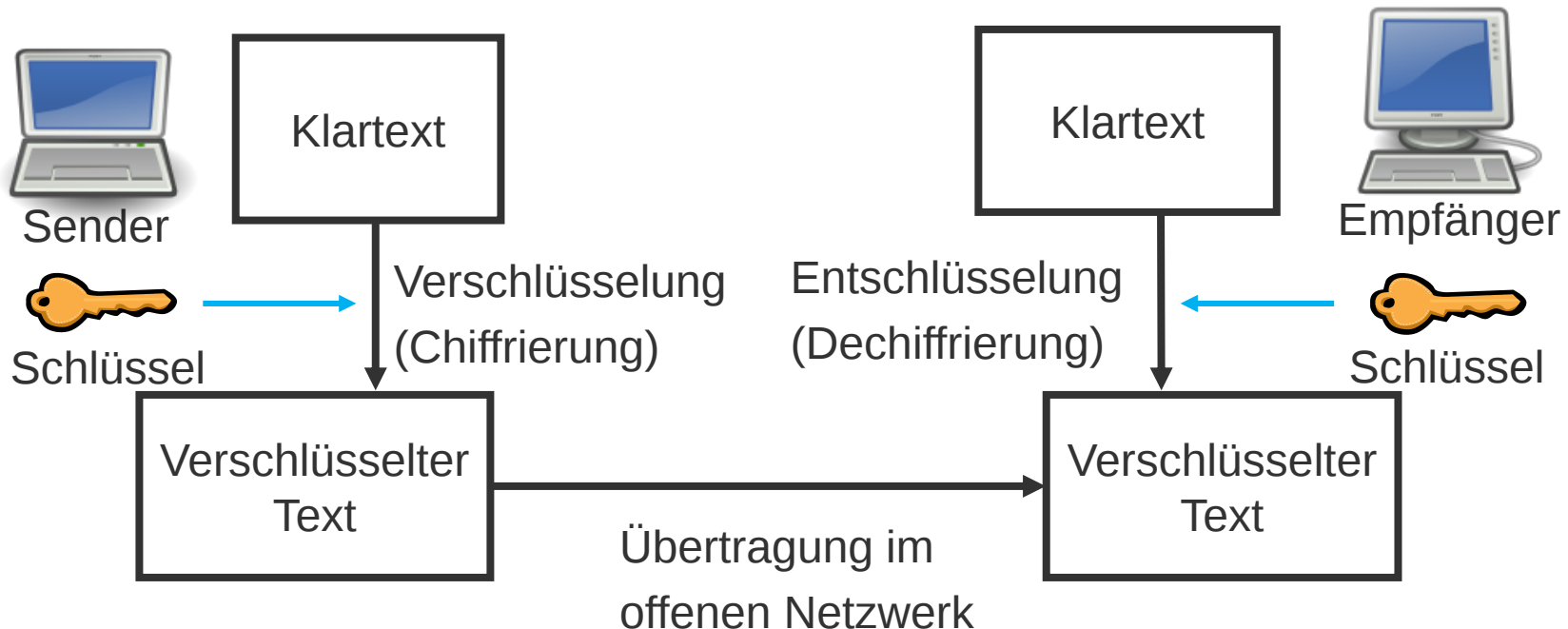
Kryptographie bietet Werkzeuge zur Absicherung der Kommunikation in offenen Netzen und Internet

Kryptographie ist mathematische Wissenschaft zur

- Verschlüsselung von Klartext („Plain Text“)
 - Umwandlung („chiffrieren“) in Schlüsseltext („Chiffretext“)
- Entschlüsselung von Schlüsseltext in Klartext

Verschlüsselungsverfahren/Chiffre ist Abbildungsvorschrift, die zusammen mit einer Geheiminformation, dem „Schlüssel“ – auswählbar aus einer astronomischen Menge ähnlicher Informationen –, angewandt wird

Sichere Kommunikation durch Kryptografie:



Sicherheit im Internet (7/7)

- System zur Ver- und Entschlüsselung „**Kryptosystem**“ besteht aus
 - einer Chiffre (Verschlüsselungsverfahren)
 - dem geheim zu haltenden Schlüssel „Secret Key“
 - einem Dechiffrierverfahren
- **Kryptokomplexität** - notwendiger Aufwand zur Ver- und Entschlüsselung
- Bei traditionellen **symmetrischen** oder **Secret-Key-Kryptosystemen** nutzen Sender und Empfänger den gleichen geheimen Schlüssel
- Bei modernen **asymmetrischen** oder **Public-Key-Kryptosystemen** werden zum Verschlüsseln und Entschlüsseln verschiedene Schlüssel benutzt