



openHPI – Sicherheit im Internet
Wie wird Kommunikation
im Internet gesichert?

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

Wie wird Kommunikation im Internet gesichert?

- Jede Kommunikation im Internet findet entlang offener Kommunikationswege statt
 - Ohne Vorkehrungen können Angreifer alle Kommunikationsinhalte mitlesen und verändern
- Können Schutz der Vertraulichkeit der Kommunikation und weitere Sicherheitsziele mittels **Verschlüsselung** gewährleisten
- Die Wissenschaft der Verschlüsselung – **Kryptographie** – existiert bereits seit Jahrtausenden
 - Damals wurden relativ einfache Verfahren zur Geheimhaltung (Verschlüsselung) eingesetzt
 - Heutzutage sind die Verschlüsselungsverfahren viel aufwändiger, um Angriffen moderner leistungsstarker Rechner standhalten zu können

Unser Programm für Kurswoche 5: Informationssicherheit durch Kryptographie



Wollen in dieser Kurswoche ein grundlegendes Verständnis von Kryptographie vermitteln und verschiedene Verschlüsselungstechniken vorstellen

Wir werden uns dazu

- **klassische Verfahren** ansehen, um grundlegende Prinzipien zu erklären,
- die beiden großen Gruppen der Verschlüsselungsverfahren, 1-Schlüssel und 2-Schlüssel Verschlüsselungen vorstellen und
- das im Internet am weitesten verbreitete **Verschlüsselungsprotokoll** betrachten.

Wir werden uns dann ansehen, wie man verschiedene **Sicherheitsziele** – Vertraulichkeit, Integrität der Nachricht und des Senders – mit Hilfe von Verschlüsselung erreichen kann und welche Infrastrukturen – **PKI** – dafür nötig sind

Sicher Kommunizieren im Internet | Sicherheit im Internet | Prof. Dr. Christoph Meinel 3