E-Mail (nur?) für Dich

Ein Unterrichtsprojekt für einen kontextorientierten und kumulativen Kompetenzerwerb zum Thema „Sichere Kommunikation über ein öffentliches Medium"

Entdeckendes Lernen:
die Protokolle durch Analyse des Netzwerkverkehrs rekonstruieren

Demonstration:
Nachricht auf dem E-Mail-Server sowie dem Kommunikationsweg mitlesen, verändern und unter falschem Absender versenden

1. Wie kommt meine **E-Mail** von meinem Computer zum Computer des Empfängers?

Protokolle:
SMTP und POP3

2. Welche **Gefahren** drohen bei der Kommunikation über ein öffentliches Medium?

mitlesen

verändern

falscher Absender

3. Wie erreiche ich **Vertraulichkeit**?

4. Wie erreiche ich **Integrität** und **Authentizität**?

Wie könnte jemand ohne den Schlüssel meine Verschlüsselung **knacken**?

Wie kann ich so verschlüsseln, dass ein **Knacken** besonders **aufwendig** wird?

Wie kann ich das **Austauschen geheimer Schlüssel vermeiden**?

verschlüsseln

symmetrisch:
Cäsar /Vigenère

asymmetrisch:
RSA

digitale Signatur:
1) Hash-Wert der Nachricht bilden
2) mit privatem Schlüssel des Absenders verschlüsseln

Anwendung:
E-Mails ver- und entschlüsseln, signieren und Signaturen prüfen

5. **Warum** sollte ich **sicher kommunizieren**?

gesellschaftliche Auswirkungen von Überwachung

Gruppenpuzzle:
Konsequenzen unsicheren Kommunizierens erkennen

Legende

Fragestellung

Fachinhalt

Aktivität(en) / Lernaufgabe(n)

A. Gramm