Christian Schindelhauer
Christian Ortolf

Freiburg, den 12. Juli 2016
Besprechung 19. Juli 2016

Übungen zur Vorlesung

# Systeme II / Rechnernetze

Sommer 2016

Blatt 11 (10 Punkte)

**AUFGABE 1:** 3 Punkte

Benutzen Sie das Programm Wireshark um den Aufruf einer Webseite einmal mit http und einmal mit https mitzuschneiden.

1. Vergleichen sie die Dauer der Kommunikation! (Zeit/RTT)
2. Was für eine Cipher Suite wurde bei der https Variante verwendet und wie viele weitere wären möglich gewesen?
3. Der Name der Cipher Suite besteht aus einer Aneinanderreihung von Abkürzungen. Erklären Sie mit je max. 2 Sätzen die Bedeutung der einzelnen Abkürzungen!

**AUFGABE 2:** 2 Punkte

Nennen und erklären Sie zwei Sicherheitsziele eines Netzwerkes und geben Sie jeweils ein Beispiel an, durch welche Art von Angriff diese verletzt werden können.

**AUFGABE 3:** 5 Punkte

Ein Server benutzt zur verschlüsselten Kommunikation das RSA-Verfahren mit folgendem Public-Key: (N, e) = (1739, 1001)

1. Wieso würde man solch einen Public-Key in der Realität nicht einsetzen?
2. Faktorisieren sie N und errechnen Sie davon ausgehend dann d.
3. Sie haben folgende Daten bei einer Kommunikation zwischen dem Server und dem Client mitgeschnitten:
   1272 666 666 1080 1272 1341 470 1382 349 437 1666 197 978
   Entschlüsseln Sie die Daten unter der Annahme, dass diese in ASCII kodiert sind.
4. Wie groß dürfen die zu verschlüsselnden Zahlen in diesem Fall maximal sein? Was passiert, wenn eine Zahl größer ist?