Christian Schindelhauer

Freiburg, den 03. Juli 2013
Besprechung 10. Juli 2013

Übungen zur Vorlesung

Systeme II / Rechnernetze

Sommer 2013

Blatt 10

AUFGABE 1: 5 Punkte

Ein Server benutzt zur verschlüsselten Kommunikation das RSA-Verfahren mit folgendem Public-Key: $(N, e) = (622579, 21113)$

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 einem Client mitgeschnitten:
   $380157 \quad 615426 \quad 92340 \quad 57197$
   Entschlüsseln Sie die Daten[1]
4. Wie groß dürfen die zu verschlüsselnden Zahlen in diesem Fall maximal sein? Was passiert wenn eine Zahl größer ist?

AUFGABE 2: 2 Punkte

Rufen Sie die Seiten *https://www.google.de/* und *https://hondo.informatik.uni-freiburg.de:13241/websys/student?lecture=systemeiisommer2013* auf und vergleichen Sie die Sicherheitszertifikate beider Seiten.

1. Betrachten Sie die Zertifikatskette und erklären Sie, warum ihr Browser einer dieser Seiten nicht vertraut.
2. Wozu dient der Fingerprint?

AUFGABE 3: 3 Punkte

Ein Unternehmen möchte den Inhalt aller http(s)-Verbindungen seiner Mitarbeiter kontrollieren. Welche Sicherheitsziele sind verletzt? Betrachten Sie:

1. http
2. https mit selbstsignierten Zertifikaten
3. https mit von einer CA signierten Zertifikaten

Beschreiben Sie für die 3 Verbindungsarten was getan werden muss um die Verbindungen abzuhören.

[1] TIPP: Die Daten sind in UTF-8 kodiert. Jede Zahl vereint 2 Bytes und steht für zwei Zeichen.