Christian Schindelhauer
Sneha Mohanty

Freiburg, den 2. Dezember 2021
Abgabeschluss 8. Dezember 2021, 23:59 Uhr UTC+1

Übungen zur Vorlesung
Rechnernetze
Winter 2021/2022
Blatt 7

Bitte laden Sie eine PDF-Datei in ILIAS hoch, andere Abgaben werden ignoriert. Schreiben Sie alle Namen und Matrikelnummern der Gruppenteilnehmer auf die Abgabe.

Aufgabe 1: RSA (7 Punkte)

Auf ILIAS werden Ihnen (ab dem 3.12.2021) drei Python-Dateien client.py, server_crypto.py und DNS.py zur Verfügung gestellt. Laden Sie diese herunter und bearbeiten Sie damit die folgenden Aufgaben. Lösen sie wie bereits auf Blatt 2 die URL: `adorabledora.ddns.net` mit Hilfe von DNS.py auf. Verwenden Sie hierbei Port 4242.

a) Teilen Sie Ihr wie folgt RZ-Kürzeln in zwei Teile und verschlüsseln Sie jeden Teil separat mit dem öffentlichen Schlüssel, den Sie über *getPub* erhalten.

   Nehmen Sie die ersten beiden Buchstaben Ihres RZ-Kürzels x und y. Berechnen Sie $27 \cdot \text{ord}(x) + y$, wobei ord : $a \mapsto 1, b \mapsto 2, ..., z \mapsto 26$ die Ordnungszahl der römischen Buchstaben im Alphabet darstellt. Den numerischen Teil nehmen Sie unverändert. Eventuell folgende Buchstaben in Ihrem RZ-Kürzel ignorieren Sie.

   Beispiel: $rz42 \rightarrow (27 \cdot \text{ord}(r) + \text{ord}(z), 42) = (512, 42)$. Verschlüsseln Sie nun 512 and 42 mit RSA und verwenden Sie den Befehl `sendData 691953 402049`, wobei 691953 und 402049 die Verschlüsselungen von 512 und 42 für den öffentlichen Schlüssel $(29, 3892153)$ sind.

b) Senden Sie mit *sendPub* ihren *Public Key* an den Server. Anschließend empfangen sie eine Verschlüsselte Zahl. entschlüssel Sie diese und geben sie diese auf der PDF an. *Beachten Sie bei Ihrem öffentlichen Schlüssel* (e, n)*, dass* $n \in [64, 1024]$. (2 Punkte)

Aufgabe 2: Sicherheitsrisiken (3 Punkte)

Werden alle Sicherheitsziele, die in der Vorlesung genannt werden, in Aufgabe 1 erreicht? Warum?