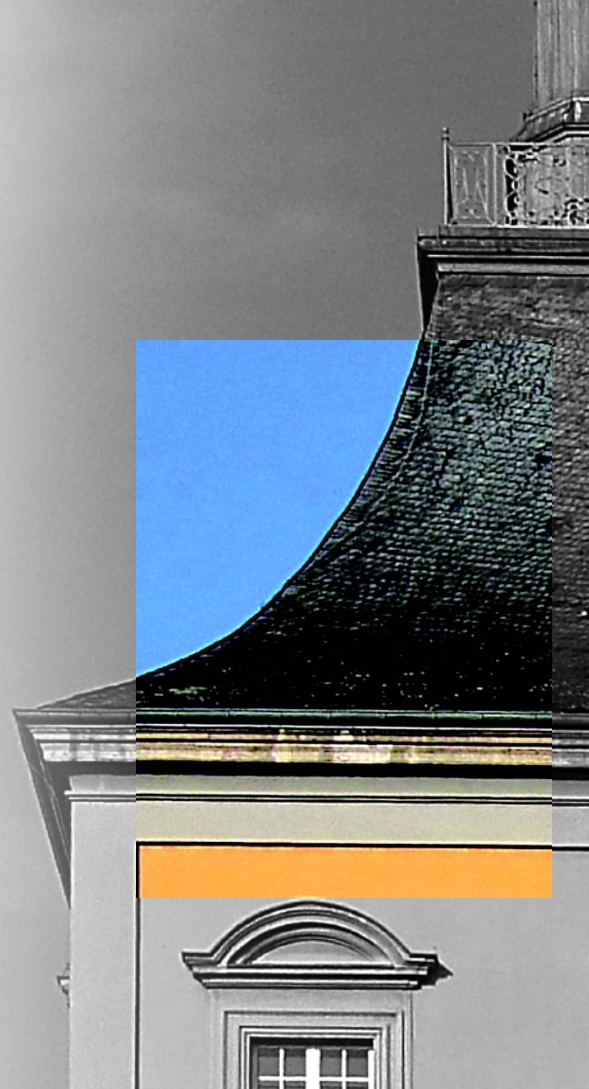
UNIVERSITÄT BONN

ÜBUNG
NETZWERKSICHERHEIT

SOMMERSEMESTER 2020

DI. 16-18 UHR



UNIVERSITÄT BONN

5. ÜBUNGSBLATT – PROJEKT 1

a) Erstellen Sie zwei RSA-Schlüsselpaare und jeweils selbst signierte Zertifikate.

b) Entwickeln Sie in C / C++ / Rust / Go (keine Skriptsprachen) eine Client-/Server-Anwendung, die folgende funktionale Eigenschaften erfüllt:

1. Client und Server kommunizieren TLS verschlüsselt über TCP und verwenden jeweils einen der Schlüssel.
2. Nach dem erfolgreichen Verbindungsaufbau senden sich Client und Server jeweils den SHA256 Fingerprint des öffentlichen Schlüssels des Kommunikationspartners und geben den empfangenen Fingerprint hexadezimal kodiert auf der Standardausgabe aus.
3. Anschließend wird die Verbindung beendet, der Server wartet dann auf die nächste Verbindung, der Client wird beendet.

c) Erstellen Sie ein Makefile für Ihr Projekt, geben Sie alle Quelldateien in Ihrer Abgabe mit ab.