Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2020-04-15
Due: 2020-04-23

SADS 2020 Problem Sheet #8

Problem 8.1: *Pretty Good Privacy (PGP)* (2+1 = 3 points)

a) Write down the sum of your matriculation number and 139626885.

b) What is the purpose of a PGP revocation certificate?

Problem 8.2: *Transport Layer Security (TLS 1.2)* (1+2+2 = 5 points)

The following questions relate to TLS 1.2 as defined in RFC 5246.

a) What is the Pseudorandom Function (PRF)?

b) TLS has a notion of a pre-master secret and a master secret. Explain why both exist and how they relate to each other and the key exchange algorithm negotiated between the two TLS peers.

c) How are keys used by the symmetric encryption algorithms derived from the master secret?

Problem 8.3: *Transport Layer Security (TLS 1.3)* (1+1 = 2 points)

The following questions relate to TLS 1.3 as defined in RFC 8446.

a) Summarize how the HMAC-based Extract-and-Expand Key Derivation Function (HDKF) works.

b) How are keys used by the symmetric encryption algorithms derived from the master secret?