technische universität
dortmund

Fakultät für Informatik
Lehrstühle 4, 12

Dimitri Scheftelowitsch, Daniel Friesel
Benedikt Maus, Christian Gemke, Thomas Krieg, Felix Homa, Rico van Endern

Wintersemester 2017/18

Rechnernetze und verteilte Systeme
Übungsblatt 12

Ausgabe: 8. Januar 2018, **Besprechung:** 16. Januar – 19. Januar 2018, **keine Abgabepflicht**

Aufgabe 12.1

(a) Was sind die Hauptsicherheitsziele?

(b) Nennen Sie weitere Sicherheitsziele. Welches Problem tritt auf, wenn man sie gleichzeitig erfüllen will?

Aufgabe 12.2

(a) Differenzieren Sie zwischen *safety* und *security*.

(b) Beschreiben Sie den Unterschied zwischen *Web of trust* und *Certification Authority*. Geben Sie für jede der Architekturen eine Beispielumsetzung an.

Aufgabe 12.3

Alice möchte Bob eine Nachricht M schicken. Wir nehmen an, dass M sehr lang (mehr als 1kB) ist. Alice kennt den öffentlichen Schlüssel K_B^+ von Bob und Bob kennt den öffentlichen Schlüssel K_A^+ von Alice. Entwerfen Sie ein Kommunikationsprotokoll mit den folgenden Eigenschaften.

- Ein Dritter kann die zwischen Alice und Bob ausgetauschten Nachrichten nicht interpretieren.
- Bob kann sicher sein, dass die Nachricht von Alice kommt.
- Bob bestätigt Alice den Empfang der Nachricht so, dass Alice sicher sein kann, dass Bob die Bestätigung geschickt hat und es sich mit Hilfe der Bestätigung mit großer Wahrscheinlichkeit nachvollziehen lässt, dass Bob die Nachricht korrekt empfangen hat.
- Der Nachrichtenaustausch soll effizient sein.

Beschreiben Sie, welche Nachrichten ausgetauscht werden und wie diese ver- und entschlüsselt werden.