Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: Zertifikate und Public-Key-Systeme

Dr. Ladan Pooyan-Weihs

Semesterwoche 09

Aufgabe 1: Zertifikate

Erstellen Sie ein kurzes Protokoll zur Zertifikaterstellung und Zertifikatüberprüfung.

Aufgabe 2: Zertifikatshierarchie

1. Welche Vorteile hat eine Zertifikatshierarchie für eine Firma und für die einzelne Benutzerin?
2. Welche Nachteile hat eine Zertifikatshierarchie für eine Firma und für den einzelnen Benutzer?

Aufgabe 3: Client-Server Authentifizierung

Studentin Alice will von Zuhause über ein lokales Netz auf einem Rechner der HSLU arbeiten. Welche Probleme können sich dabei ergeben? Erstellen Sie ein kurzes einfaches Protokoll, um eine sichere Authentifizierung zu ermöglichen.

Aufgabe 4: PGP

Beschreiben Sie den Begriff «Key escrow» (Schlüsselhinterlegung).

Aufgabe 5: GPA

Warum wird die Kommunikation auf Dark Web häufig mit Hilfe von GPA realisiert?

Viel Vergnügen!