Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: Protokolle I

Prof. Dr. Josef F. Bürgler
Dr. Ladan Pooyan-Weihs

Semesterwoche 07

Aufgabe 1: Diffie-Hellmann-Schlüsselaustausch

Im Unterricht wurde das Protokoll Diffie-Hellmannsicher vorgeführt. Kann ein Angreifer Namens Mr. X das System angreifen, falls er die Zahlen α und β kennen wurde? Begründen Sie Ihre Antwort.

Aufgabe 2: Schlüsselaustausch

Sie haben im Unterricht ein Protokoll für hybride Verschlüsselung mit unsicherem Kanal kennengelernt. Überlegen sie sich, wie ein anderes Verfahren für diese Art der Verschlüsselung funktionieren könnte?

Aufgabe 3: Blinde Signatur

Führen Sie zu Zweit die blinde Signatur durch. Protokollieren Sie das Vorgehen und zeigen Sie, wie der Signierer die Nachricht berechnen kann, welche er (blind) signiert!

Aufgabe 4: Bit-Commitment

Alice leitet die Vertriebsabteilung einer IT-Firma. Sie bereitet eine Offerte mit ihrem Team vor, um an einem digitalen Ausschreibungsprozess teilzunehmen. Als Protokoll zum Anreichen der

Offerten wurde Bit-Commitmnet allerdings mit einem Bit *b* der Länge eins (1) festgelegt. Wie kann Alice sicher sein, dass Bob (ein Mitbewerber) das Bit *b* nicht berechnen kann?

Viel Vergnügen!