Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: Protokolle

Prof. Dr. Josef F. Bürgler

Dr. Ladan Pooyan-Weihs

Semesterwoche 08

Die Lösung der Aufgaben besteht darin, dass Sie ein einfaches Beispiel angeben. Ein Auszug aus dem Buch «Moderne Verfahren der Kryptographie» über *Anonymität* befindet sich im Ordner SW08 auf ILLIAS, den Sie für diese Übung lesen sollten.

Aufgabe 1: Dining-Cryptographers

Ziehen Sie das Protokoll *Dining-Cryptographers* im Falle einer Dreiergruppe einige Male durch, indem sie das Protokoll mit einem Schiedsrichter überprüfen: es sollen also vier Leute in einer Gruppe arbeiten! Aufgabe: erstellen Sie ein kurzes Protokoll!

Aufgabe 2: Anonymes Senden

Überlegen Sie sich ein Beispiel für den zweiten Paragraphen in Abschnitt 6.1! Aufgabe: erstellen Sie ein kurzes Protokoll (es soll ein von Ihnen durchgeführtes Experiment beschreiben)!

Aufgabe 3: MIXe

Spielen das anonyme Versenden von Nachrichten wie in Abschnitt 6.2 beschrieben anhand einfacher Zahlenbeispiele durch. Aufgabe: erstellen Sie ein kurzes Protokoll (es soll ein von Ihnen durchgeführtes Experiment beschreiben)!

Aufgabe 4: Anonymität

Was ist «traffic analysis»? Welche Art von Anonymität, die Sie gelernt haben, kann eine Lösung dagegen anbieten? Begründen Sie Ihre Antwort.

Aufgabe 5: Secret Splitting / Geteiltes Geheimnis

Verteilen Sie das Geheimnis 01011001 auf drei Leute! Protokollieren Sie das Vorgehen und zeigen Sie, wie man das Geheimnis rekonstruiert.

Aufgabe 6: (2,3)-Schwellenwertproblem

Das Geheimnis *M* wird mit den drei Zufallszahlen R_1, R_2, R_3in drei Teilgeheimnisse aufgeteilt. Das Teilgeheimnis $M_1 = (M_{11}, M_{12}, M_{13}) = (R_1 \oplus M, R_2, R_3)$ ist gegeben.

1. Definieren Sie M_2 und M_3 .
2. Rekonstruieren Sie *M* nur mit zwei Teilgeheimnissen.

Aufgabe 7: Secret Sharing Schema: Wie hoch ist das Durchschnittsgehalt?[1]

Alice, Bob und Carol wollen jedoch nicht verraten, wie viel Geld sie verdienen. Sie möchten jedoch den Durchschnitt ihrer Gehälter berechnen, um mit Hilfe dieses Wertes zu ersehen, ob sie mit ihrem Gehalt zufrieden sind oder ob sie bei der nächsten Gehaltserhöhung kräftig zulangen sollten. Zunächst gehen sie mit einem kryptographischen Protokoll vor. Alice startet. Sie wählt eine Zufallszahl *r* und addiert ihr Gehalt *a* dazu. Diesen Wert schickt sie an Bob weiter. Er erhöht diesen Wert um sein Gehalt *b*. Dann fügt Carol Ihr Gehalt *c* dem vertraulichen Wert $r + a + b$ hinzu und gibt ihn an Alice zurück.

1. Wie berechnet nun Alice den Durchschnitt ihrer Gehälter?
2. Kann eine/r der drei Teilnehmenden das Gehalt einer/s anderen bestimmen? Begründen Sie bitte Ihre Antwort?
3. Welche Werte kennt Bob?

Aufgabe 8: Threshold-Verfahren

Alice teilt ein Geheimnis *S* mit einem Polynom des 2. Grades mit. Die Zahl *S* ist die y-Achsenabschnitt *(0, S),* die das Geheimnis darstellt. Als Teilgeheimnisse sind drei (3) verschiedene Punkte *(3, 2), (4, 1), (5, 2)* bekannt. Wie rekonstruieren Sie das Geheimnis?

Viel Vergnügen!

[1] Basiert auf dem Buch « Moderne Verfahren der Kryptographie» von A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter