Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

I.BA_MOVK_MM – Kryptographie

Übung: ePayment

Dr. Ladan Pooyan-Weihs

Semesterwoche 12

Aufgabe 1:

Ein Betrüger möchte eine Bank, die Protokoll Nr. 4 benutzt, dazu bringen, blind eine 100-CHF-Münze zu signieren, seinem Konto aber nur einen Schweizer Franken zu belasten. Dazu erzeugt er 99 Münzen vom Wert CHF 1 und eine 100-CHF-Münze.

a) Wie gross ist die Wahrscheinlichkeit dafür, dass die Bank blind die 100-CHF-Münze signiert?
b) Wie kann der Bank verhindern, dass der Kunde einen Betrugsversuch unternimmt?

Aufgabe 2:

Das Protokoll von E-Cash entwickelt von der Firma Digicash sieht eine zufällig gewählte Seriennummer S für jede eMünze vor. Sollte S zufällig gewählt werden oder sollte S wie die Zahl X im Wahlzettel für eVoting (Vorlesung SW11) von einer bestimmten Struktur sein? Begründen Sie Ihre Antwort?

Aufgabe 3:

Lesen Sie die Dokumente unter dem Link unten und beantworten Sie die folgenden Fragen:

1. Was ist ein Fiatgeld?
2. Aus welchem Grund wurde zum ersten Mal eine Währung als Fiatgeld eingeführt? Wann war das?
3. Nennen Sie zwei weitere Beispiele für das Fiatgeld.

Link auf ILIAS: SW12

Aufgabe 4:

Wie viele Bit muss die zufällig generierte Seriennummer einer E-Münze lang sein, damit die Wahrscheinlichkeit für eine zufällige Übereinstimmung von zwei Nummern kleiner ist als die Wahrscheinlichkeit, bei zwei aufeinander folgenden Ziehungen im Lotto (6 aus 49) sechs Richtige zu tippen? Tipp: Berechnen Sie zuerst die Wahrscheinlichkeit, mit einer zufällig erzeugten Seriennummer eine vorgegebene Zahl fester Länge zu treffen. Bestimmen Sie dann deren Länge n.

Aufgabe 5:

Sei Alices Identitätsinformation *UID = 1000*. Ist die folgende Gleichung korrekt?

$$1000 = 9008 \oplus 8408$$

Viel Vergnügen!