Hochschule für
Technik und Wirtschaft
des Saarlandes
University of Applied Sciences

Studiengang Kommunikationsinformatik (Master)
Prof. Dr.–Ing. Damian Weber

Sicherheit und Kryptographie – Wiederholungsübung

Aufgabe 1 (Algebraische Strukturen)

Was bedeuten die Begriffe *Gruppe* und *Körper*?

Aufgabe 2 (Gruppen)

Sei G eine Gruppe, $a \in G$ ein Element und n die Elementordnung von a.

Zeigen Sie: die Elementordnung von a^{-1} ist ebenfalls n.

Hinweis: zeigen Sie zunächst, daß die Ordnung von a^{-1} höchstens n ist, danach, daß sie nicht kleiner als n ist.

Aufgabe 3 (Untergruppen)

Gegeben sei der Körper $\mathbf{F}_p$ mit p Elementen, wobei p Primzahl. Es sei q ein Teiler von $p-1$.

Zeigen Sie: alle q–ten Potenzen in $\mathbf{F}_p \setminus \{0\}$ bilden eine Untergruppe der Gruppe $(\mathbf{F}_p \setminus \{0\}, \cdot)$

Aufgabe 4 (Modulare Arithmetik)

Ist $3^{2006} - 2$ durch 7 teilbar?

Aufgabe 5 (Diffie–Hellman–Protokoll)

Alice und Bob führen das Diffie–Hellman–Protokoll im Körper $\mathbf{F}_{11}$ aus. Sie wählen als Erzeuger $g = 7$. Alice wählt als geheime Zufallszahl $a = 9$, Bob $b = 7$. Welcher gemeinsame geheime Schüssel wird von beiden berechnet?

Hinweis: Potenzierungstabelle in $\mathbf{F}_{11}$

i	1	2	3	4	5	6	7	8	9	10
7^i	7	5	2	3	10	4	6	9	8	1

Aufgabe 6 (Logarithmen–Basis)

Lösen Sie das Problem

$$2^x \equiv 9 \mod 11$$

mit Hilfe der obigen Potenzierungstabelle.

Aufgabe 7 (Quadratische Reste)

a) Zeigen Sie: 10 ist ein quadratischer Nichtrest mod 11.

b) Begründen Sie: für Primzahlen $p \geq 3$ kann ein quadratischer Rest y kein Erzeuger in $\mathbf{F}_p$ sein.

c) Ist die Aussage b) für $p = 2$ auch richtig?

Aufgabe 8 (Körpererweiterung)

Wie kann man den Körper $\mathbf{F}_{11}$ zum Körper $\mathbf{F}_{11^2} = \mathbf{F}_{11}(\alpha)$ erweitern? Geben Sie unter Benutzung der vorigen Aufgabe ein geeignetes Polynom an.

Aufgabe 9 (Strukturen in symmetrischen Verfahren)

Die folgenden C/C++-Operationen auf zwei 32-Bit-Werten `unsigned int a, b` sollen durch geeignete algebraische Strukturen beschrieben werden.

Nennen Sie die richtige Struktur (Gruppe, Ring, Körper, Vektorraum) die Bezeichnung ihrer Menge (z.B. $\mathbf{F}_2^{32}$) und die zugehörige Operation.

a) Addition `a+b`

b) XOR (exklusiv-oder) `a^b`

c) Shift nach links um b Stellen `a<<b`

d) Rotieren nach links um b Stellen `ROL(a,b)`

Aufgabe 10 (Elliptische Kurven)

Betrachten Sie die Kurve

$$E: \quad y^2 \equiv x^3 + x \mod 5.$$

a) Prüfen Sie, ob E eine gültige elliptische Kurve darstellt.

b) In welchem Intervall liegt nach dem Satz von Hasse die Anzahl der Punkte $|E|$?

c) Bestimmen Sie $|E|$.

d) Erstellen Sie die Verknüpfungstabelle der Gruppe $(E, +)$.

e) Bestimmen Sie für jeden Punkt $P \in E$ die Elementordnung von P.
Hinweis: die Formeln zur Punktaddition sind hierfür nicht erforderlich.