htw saar

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 (Modulare Arithmetik)

Ist $3^{2016} - 1$ durch 7 teilbar?

Aufgabe 3 (RSA)

Berechnen Sie zu den geheimen RSA–Parametern von Alice

$$p = 5, \quad q = 11, \quad d = 27$$

den zugehörigen öffentlichen Schlüssel.

Jemand möchte Alice die Nachricht $m = 7$ zukommen lassen und verschlüsselt die Nachricht mit ihrem öffentlichen Schlüssel. Welcher Wert wird über den öffentlichen Kanal versendet?

Alice kann mit Hilfe ihrer geheimen Parameter p und q die verschlüsselte Nachricht mod p und mod q entschlüsseln und danach mit den chinesischen Restsatz zusammensetzen. Führen Sie diesen Vorgang für die verschlüsselte Nachricht aus.

Aufgabe 4 (Diffie–Hellman–Protokoll)

Alice und Bob führen das Diffie–Hellman–Protokoll modulo 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 5 (Pollard–ϱ)

Gegeben sei folgende Problem des diskrete Logarithmus

$$5^x \equiv 13 \mod 23.$$

Reduzieren Sie das Problem auf den Faktor $q = 11$ und führen Sie das Pollard–ϱ–Verfahren zum Berechnen diskreter Logarithmen mit den Startwerten $k = 1$, $l = 1$ aus, um x mod 11 zu berechnen. (Ergebnis: $x \equiv 3 \mod 11$).

Reduzieren Sie das Problem auf den Faktor $q = 2$ und erhalten Sie das Ergebnis $x \mod 2$ durch Ausprobieren.

Setzen Sie das Ergebnis mit dem chinesischen Restsatz mod 22 zusammen.

Aufgabe 6 (Körpererweiterung)

Wie kann man den Körper $\mathbf{F}_2$ zum Körper $\mathbf{F}_{2^3} = \mathbf{F}_2(\alpha)$ erweitern? Geben Sie ein geeignetes Polynom an und listen Sie die 8 Elemente auf.

Aufgabe 7 (Elliptische Kurven)

Betrachten Sie die Kurve

$$E: \quad y^2 \equiv x^3 + 5x - 1 \mod 7.$$

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 $|E|$ (Ergebnis $|E| = 4$).

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.