htw saar

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

Sicherheit und Kryptographie – Wiederholungsübung 1 - Lösungstipps

Aufgabe 1 (Algebraische Strukturen)

Siehe Handout *Definitionen algebraischer Strukturen.*

Aufgabe 2 (Modulare Arithmetik)

Benutze kleinen Fermat'schen Satz.

Aufgabe 3 (RSA)

RSA–Verfahren anwenden.

Beim Entschlüsseln mod p und mod q reduzieren und dort kleinen Fermat'schen Satz anwenden.

Aufgabe 4 (Diffie–Hellman–Protokoll)

Kleinen Fermat'schen Satz anwenden und Ergebnis aus Potenzierungstabelle ablesen.

Aufgabe 5 (Pollard–ϱ)

Folgendefinition anwenden und nachrechnen.

Aufgabe 6 (Körpererweiterung)

Siehe $\mathbf{F}_{2^8}$ bei AES.

Aufgabe 7 (Elliptische Kurven)

Hasse–Intervall,

y–Werte zu allen x–Werten ausrechnen, die ein Quadrat liefern

Elementordnung: kleinster Wert $n \in \mathbf{N}$ mit $n \cdot P = \mathcal{O}$