

Übungen zur Vorlesung Kryptographie

Blatt 2

Aufgabe 5: (Einheitengruppen)

- (a) Bestimmen Sie alle Elemente von Z_9^* . Welchen Wert hat die Ordnung von Z_9^* ? Was ist der Wert von $\varphi(9)$? Bestimmen Sie alle Untergruppen von Z_9^* .
- (b) Was sind die Elemente von Z_p^* , wenn p eine Primzahl ist?
- (c) Für wieviele Zahlen n zwischen 0 und 105 gilt $\text{ggT}(n, 105) = 1$?

Aufgabe 6: (Klein- φ macht auch Mist)*Diese Aufgabe bitte ohne Computer lösen!*

- (a) Berechnen Sie das inverse Element von 150 in Z_{301}^* und das inverse Element von 89 in Z_{144}^* von Hand mittels des erweiterten euklidischen Algorithmus.
- (b) Bestimmen Sie alle $n \in \mathbb{N}$, so dass $\varphi(n) = 2$. Begründen Sie auch, warum das wirklich alle sind!
- (c) Zeigen Sie, dass $\varphi(n)$ immer gerade ist für $n \geq 3$.

Aufgabe 7: (Euler-Fermat benutzen)*Diese Aufgabe bitte ohne Computer lösen!*

- (a) Was ist die letzte Ziffer von 999^{999} ?
- (b) Berechnen Sie die letzten beiden Dezimalziffern von $2^{1\,000\,003}$.

Aufgabe 8: (Amazon und der chinesische Restsatz)*Bitte ohne Computer lösen!*

Ein hochqualifizierter, teamfähiger, motivierter und preiswerter Lagerarbeiter der Firma Amazon packt m Alexas in 16er-Kartons. Dabei bleiben 6 Alexas übrig. Daher packt er alles wieder aus und packt die m Alexas nun in 25er-Kartons. Dabei bleiben 7 Alexas übrig. Daher packt er erneut alles wieder aus und packt die m Alexas nun in 49er-Kartons. Diesmal bleiben 8 Alexas übrig. Es sind insgesamt weniger als 10 000 Alexas. Was ist der Wert von m ?

(Es ist OK, für die konkreten Additionen und Multiplikationen von Zahlen einen Taschenrechner oder Computer zu nutzen.)

Abgabe bis Mittwoch 28.4.2021 bis 14 Uhr per Email an den Tutor.

Bitte auf jeder Abgabe das Tutorium angeben!

Jan Jan-Philipp Brünger
Leonard Simon Ellinghaus
Kallias Stoupas

jbruenger@techfak.de
lellinghaus+krypto@techfak.de
kstoupas+krypto@techfak.de