Übungen zur Vorlesung Kryptographie

Blatt 2

Bitte alle Aufgaben von Hand lösen (ohne `sagemath`, `python` *usw). Computerlösungen zählen diesmal ausnahmsweise nicht. Zwischenrechnungen wie* $17 \cdot 27$ *oder* $168 - 73$ *dürfen Sie natürlich mit Computer, Taschenrechner, Handy-App, ... berechnen.*

Aufgabe 5: (Klein-φ macht auch Mist)
(a) Bestimmen Sie alle Elemente von Z_{12}^*. Welchen Wert hat die Ordnung von Z_{12}^*? Was ist der Wert von $\varphi(12)$? Bestimmen Sie alle Untergruppen von Z_{12}^*.

(b) Was sind die Elemente von Z_p^*, wenn p eine Primzahl ist?

(c) Für wieviele Zahlen n mit $0 \leq n \leq 105$ gilt $\mathrm{ggT}(n, 105) = 1$?

Aufgabe 6: (Mehr zu Einheitengruppen)
(a) Berechnen Sie das inverse Element von 168 in Z_{503}^* und das inverse Element von 144 in Z_{233}^* von Hand mittels des erweiterten euklidischen Algorithmus.

(b) Bestimmen Sie alle $N \in \mathbb{N}$, so dass die jeweilige Einheitengruppe Z_N^* genau vier Elemente hat. Begründen Sie, warum das wirklich alle sind!

Aufgabe 7: (Euler-Fermat benutzen)
(a) Was ist die letzte Ziffer von $999^{(99^9)}$?

(b) Berechnen Sie die letzten beiden Dezimalziffern von $23^{1\,000\,002}$ von Hand.

Aufgabe 8: (Das bekloppte Büro)
(a) Welche der folgenden fünf Objekte sind Ringe, welche nicht? Und welche sind Körper, welche nicht? Falls nein, warum nicht?

$$(Z_5, +, \cdot),\ (Z_{10}, +, \cdot),\ (\{0,1\}, \mathrm{AND}, \mathrm{XOR}),\ (\mathbb{R}^{2\times 2}, +, \cdot),\ \left(\left\{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\right\}, +, \cdot\right)$$

(b) In der Univerwaltung gibt es drei Angestellte, deren Tische nebenaneinanderstehen. Also sitzt eine in der Mitte, eine rechts, eine links. Rechts und links neben den Tischen stehen Papierkörbe. Die ausufernde Bürokratie hat bereits so sehr an den Nerven der Uniangestellten gezerrt, dass Sie ausrasten, wenn mehr als eine Akte auf Ihrem jeweiligen Schreibtisch liegt. Sie werfen in diesem Fall jeweils eine Akte nach links und nach rechts. Finden Sie alle Möglichkeiten, wie insgesamt zwei oder drei Akten auf den drei Tischen liegen können, ohne dass jemand ausrastet.

Fortsetzung auf Seite 2

Diese Möglichkeiten bilden nun die Elemente einer Gruppe G. Die Verknüpfung $\oplus$ ist einfach "tischweise Addition, dann abwarten, bis niemand mehr ausrastet". So führt z.B. $(1,1,0) \oplus (0,1,1)$ zu der Situation $(1,2,1)$. Also rastet jetzt die mittlere aus, danach ergibt sich $(2,0,2)$. Nun rasten beide außen aus, zwei Akten landen daher in den Papierkörben, und es ergibt sich $(0,2,0)$. Die mittlere rastet wieder aus, also ergibt sich $(1,0,1)$, und das ist stabil. Also $(1,1,0) \oplus (0,1,1) = (1,0,1)$. Ist $(G, \oplus)$ eine Gruppe? Begründen Sie Ihre Antwort. Falls "ja", was ist das neutrale Element?

Nun wir betrachten die Menge G' aller Möglichkeiten, wie insgesamt null oder eine oder zwei oder drei Akten auf den drei Tischen liegen können, ohne dass jemand ausrastet. Welche Elemente enthält G'? Ist $(G', \oplus)$ eine Gruppe? Begründen Sie Ihre Antwort. Falls "ja", was ist das neutrale Element?

Es ist ein Fakt, dass die Reihenfolge der Ausraster das Endergebnis der Gruppenoperation $\oplus$ nicht beeinflusst. Das muss man eigentlich beweisen, aber das müssen Sie hier nicht tun.

Abgabe bis Mittwoch 23.4.2025 bis 14 Uhr per Email an die Tutorin.
Bitte auf jeder Abgabe das Tutorium angeben!

Lisa Harms lharms+krypto@techfak.de
Lisa Henetmayr lhenetmayr+krypto@techfak.de