Dr. Dirk Frettlöh 17.4.2024

Übungen zur Vorlesung Kryptographie

Blatt 2

Bitte alle Aufgaben von Hand lösen (ohne `sagemath`, `python` *usw). Computerlösungen zählen diesmal ausnahmsweise nicht. Rechnungen wie* $234 + (-56)$ *oder* $7 \cdot 47$ *oder* $41778 \bmod 400$ *dürfen Sie mit dem Rechner oder sagemath oder Taschenrechner oder Handy-App oder... ausführen und müssen das nicht extra hinschreiben. Ansonsten wollen wir aber den Rechenweg sehen.*

Aufgabe 5: (Einheitengruppen)
(a) Was sind die Elemente von Z_7^*? Was sind jeweils ihre inversen Elemente?

(b) Was sind die Elemente von Z_{24}^*? Was sind jeweils ihre inversen Elemente?

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

Aufgabe 6: (Inverse berechnen)
(a) Berechnen Sie das inverse Element von 250 in Z_{501}^* und das inverse Element von 89 in Z_{144}^* 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: (Amazon und der chinesische Restsatz)
Ein hochqualifizierter, teamfähiger, motivierter und sehr preiswerter Lagerarbeiter der Firma Amazon packt m Alexas in 16er-Kartons. Dabei bleiben 2 Alexas übrig. Daher packt er alles wieder aus und packt die m Alexas nun in 25er-Kartons. Dabei bleiben 3 Alexas übrig. Daher packt er erneut alles wieder aus und packt die m Alexas nun in 49er-Kartons. Diesmal bleiben 4 Alexas übrig. Es sind insgesamt weniger als 10 000 Alexas. Was ist der Wert von m? Und welche Größe k müssten die Kartons haben, damit all diese Alexas in ℓ Kartons der Größe k passen?

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?

$$(Z_3, +, \cdot),\ (Z_9, +, \cdot),\ (\{0,1\}, \mathrm{XOR}, \mathrm{AND}),\ (\mathbb{R}^{2\times 2}, \cdot, +),\ \left(\left\{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\right\}, +, \cdot\right)$$

Fortsetzung Seite 2

(b) In der Univerwaltung gibt es drei Angestellte, deren Tische nebeneinanderstehen. 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 mehr Akten auf den drei Tischen liegen können, ohne dass jemand ausrastet.

Diese Möglichkeiten bilden nun die Elemente einer eine 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 mehr 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 Dienstag 23.4.2024 bis 23:59 Uhr per Email an den Tutor.
Bitte die Abgaben so nennen: [techfakaccount]-bl$n$.pdf, also z.B. `dfrettloeh-bl2.pdf`, oder `dfrettloeh+mnebel-bl2.pdf`.

Jakob Niermann	Mi 16 Uhr in T2-233	janiermann+krypto@techfak.de
Enrico di Gaspero	Do 16 Uhr in U2-216	edigaspero+krypto@techfak.de
Lisa Henetmayr	Fr 10 Uhr in X-E0-205	lhenetmayr+krypto@techfak.de
Richard Freidhof	Fr 12 Uhr in T2-141	rfreidhof+krypto@techfak.de