Dr. Dirk Frettlöh 11.4.2022

Übungen zur Vorlesung Kryptographie

Blatt 2

Bitte alle Aufgaben von Hand lösen (ohne `sagemath`, `python` *usw). Computerlösungen zählen diesmal ausnahmsweise nicht.*

Aufgabe 5: (Einheitengruppen)
(a) Was sind die Elemente von Z_7^*? Was sind jeweils ihre inversen Elemente? Was ist der Wert von $\varphi(7)$?

(b) Was sind die Elemente von Z_{24}^*? Was sind jeweils ihre inversen Elemente? Was ist der Wert von $\varphi(24)$?

(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: (Euler-Fermat benutzen)
(a) Berechnen Sie $3^{1\,000\,003} \bmod 101$ von Hand.

(b) Berechnen Sie die letzten beiden Dezimalziffern von $23^{1\,000\,005}$ von Hand.

Aufgabe 8: (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?

Für die einzelnen Additionen, Subtraktionen und Multplikationen können Sie gerne auch einen Computer oder Taschenrechner nutzen. Wir möchten aber den genauen Rechenweg sehen.

Abgabe bis Montag 25.4.2022 bis 14 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jan-Philipp Brünger jbruenger@techfak.de
Simon Hahm shahm+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de