Aufgabenblatt

Übung zur Kryptographie Wintersemester 2017/18

Priv. Doz. Dr. Markus Kirschmer
Christoph Schönnenbeck, M. Sc.

Bitte geben Sie die bearbeiteten Aufgaben am Montag, 16.10.2017, zu Beginn der Übung um 12:15 Uhr ab. Es darf zu zweit abgegeben werden.

Aufgabe 1 (4 Punkte) *Es seien a, b, c positive ganze Zahlen. Zeigen Sie mit Hilfe der Definition:*

a) Aus $a \mid b$ und $b \mid a$ folgt $a = b$.

b) Es gilt $ggT(c \cdot a,\, c \cdot b) = c \cdot ggT(a,\, b)$.

c) Es gilt $ggT(a,\, b) = ggT(a - k \cdot b,\, b)$ für alle $k \in \mathbb{Z}$.

d) Ist a gerade und b ungerade, so ist $ggT(a,\, b) = ggT(a/2,\, b)$.

Aufgabe 2 (4 Punkte) *a) Berechnen Sie $g := ggT(114, 72)$ sowie ganze Zahlen a und b mit $114a + 72b = g$.*

b) Bestimmen Sie das multiplikative Inverse von $17 + 23\,\mathbb{Z}$ in $\mathbb{Z}\,/23\,\mathbb{Z}$.

c) Es sei $A := \begin{pmatrix} 5 & 7 \\ 4 & 3 \end{pmatrix}$. Betrachten Sie A zunächst als Element von $\mathbb{Z}^{2\times 2}$ und dann als Element von $(\mathbb{Z}\,/9\,\mathbb{Z})^{2\times 2}$ und bestimmen Sie, falls möglich, ein Inverses von A in dem jeweiligen Ring.

Aufgabe 3 (4 Punkte) *a) Es sei $R := \mathbb{Z}\,/26\,\mathbb{Z}$. Zu $a \in R^*,\ b \in R$ definiere*

$$e_{a,b} : R \to R; x \mapsto ax + b$$

wie in der Vorlesung. Bestimmen Sie $c,\ d \in R$, so dass $e_{c,d} = e_{a,b}^{-1}$.

b) Das folgende Chiffrat wurde mit dem Caesarverfahren, d.h. mit Hilfe einer Funktion $e_{a,b}$ wie oben, verschlüsselt, wobei wir wie üblich A mit $0+26\,\mathbb{Z}$, B mit $1+26\,\mathbb{Z}$ etc. identifizieren:

TKUHSIURRPUKTHUOUHVGRCYPUTUR

Dechiffrieren Sie den Text mittels einer Frequenzanalyse und bestimmen Sie a und b.