Übungen zur Kryptologie 1 Wintersemester 05/06

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 2

Aufgabe 6 (mündlich)

Verschlüsseln Sie den Text DREIEINS mittels einer

a) additiven Chiffre mit dem Schlüssel $k = 13$,

b) affinen Chiffre mit dem Schlüssel $k = (17, 6)$,

c) Vigenère-Chiffre mit dem Schlüssel $k =$TIM,

d) Hill-Chiffre mit der 4×4-Schlüsselmatrix aus der Vorlesung.

Aufgabe 7 (mündlich)

Bestimmen Sie die Anzahl der Lösungen $x \in \{0, \ldots, m-1\}$ der Kongruenzgleichung

$$ax \equiv_m b$$

in Abhängigkeit von $\mathrm{ggT}(a, m)$ und b. Betrachten Sie zunächst den Fall $b = 0$.

Aufgabe 8 (mündlich)

Bestimmen Sie für $m = 6, 8$ und 26 die Anzahl der invertierbaren 2×2-Matrizen über $\mathbb{Z}_m$.
Hinweis: Benutzen Sie Aufgabe 10 und den Chinesischen Restsatz.

Aufgabe 9 (mündlich)

a) Zeigen Sie, dass für jede selbstinverse Matrix A über $\mathbb{Z}_{26}$ gilt: $\det(A) \equiv_{26} \pm 1$.

b) Bestimmen Sie die Anzahl der selbstinversen 2×2-Matrizen über $\mathbb{Z}_{26}$.

Aufgabe 10 (schriftlich, 10 Punkte)

a) Zeigen Sie, dass im Fall p prim genau $(p^2 - 1)(p^2 - p)$ invertierbare 2×2-Matrizen über $\mathbb{Z}_p$ existieren.

b) Bestimmen Sie die Anzahl aller invertierbaren $k \times k$-Matrizen über $\mathbb{Z}_p$.

Hinweis: Benutzen Sie, dass eine $k \times k$-Matrix über $\mathbb{Z}_p$, p prim, genau dann invertierbar ist, wenn die Zeilen der Matrix linear unabhängige Vektoren (über $\mathbb{Z}_p$) sind.

Abgabe am 1.11.2005 zu Beginn der Übung.