Übungen zur Kryptologie 1

Johannes Köbler/Olaf Beyersdorff

Sommersemester 2002

Übungsblatt 2

Aufgabe 6
Verschlüsseln Sie den Text KLARTEXT mittels einer
a) additiven Chiffre mit dem Schlüssel \( k = 13 \),
b) affinen Chiffre mit dem Schlüssel \( k = (25, 2) \),
c) Vigenère-Chiffre mit dem Schlüssel \( k = \text{TOP} \),
d) Hill-Chiffre mit der \( 4 \times 4 \)-Schlüsselmatrix aus der Vorlesung.

Aufgabe 7
Bestimmen Sie die Anzahl der Lösungen \( x \in \{0, \ldots, m-1\} \) der Kongruenzgleichung
\[ ax \equiv_m b \]
in Abhängigkeit von \( \gcd(a, m) \) und \( b \). Betrachten Sie zunächst den Fall \( b = 0 \).

Aufgabe 8
Bestimmen Sie für \( m = 6, 9 \) und 26 die Anzahl der invertierbaren \( 2 \times 2 \)-Matrizen über \( \mathbb{Z}_m \).

Aufgabe 9
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 \( 2 \times 2 \)-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 \( 2 \times 2 \)-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.