Übungen zur Kryptologie 1 Sommersemester 2002

Johannes Köbler/Olaf Beyersdorff

Übungsblatt 1

Aufgabe 1

Der Kryptotext BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD wurde durch eine additive Chiffre generiert. Entschlüsseln Sie ihn.

Aufgabe 2

Berechnen Sie:

a) $7503 \bmod 81$,

b) $(-7503) \bmod 81$,

c) $81 \bmod 7503$ und

d) $(-81) \bmod 7503$.

Aufgabe 3

Bestimmen Sie die Anzahl der Schlüssel in der affinen Chiffre mit den Moduln $m = 30, 100$ und 1225.

Aufgabe 4

Bestimmen Sie alle involutorischen Schlüssel k (d.h. E_k ist involutorisch) in der additiven Chiffre mit dem Modul $m = 26$.

Aufgabe 5 (schriftlich, 10 Punkte)

a) Sei $k = (b, c)$ ein Schlüssel der affinen Chiffre. Zeigen Sie, dass E_k genau dann involutorisch ist, wenn $b^2 \equiv_m 1$ (b ist selbstinvers in $(\mathbb{Z}_m, \odot_m)$) und $c(b+1) \equiv_m 0$ gilt.

b) Bestimmen Sie alle involutorischen Schlüssel in der affinen Chiffre mit dem Modul $m = 15$.

c) Wie viele involutorische Schlüssel existieren in der affinen Chiffre, wenn der Modul $m = pq$ das Produkt zweier Primzahlen p und q ist?