

Übungsblatt 1

Aufgabe 1 (mündlich)

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

Aufgabe 2 (mündlich)

Berechnen Sie:

- a) $2602 \bmod 81$,
- b) $(-2602) \bmod 81$,
- c) $81 \bmod 2606$ und
- d) $(-81) \bmod 2606$.

Aufgabe 3 (mündlich)

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

Aufgabe 4 (mündlich)

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

Aufgabe 5 (mündlich)

- a) Sei $k = (b, c)$ ein Schlüssel der affinen Chiffre. Zeigen Sie, dass E_k genau dann involutorisch ist, wenn $b^2 \equiv_m 1$ und $c(b+1) \equiv_m 0$ gilt.
- b) Bestimmen Sie alle involutorischen Schlüssel in der affinen Chiffre mit dem Modul $m = 35$.
- c) Wie viele involutorische Schlüssel existieren in der affinen Chiffre über einem Alphabet mit m Zeichen, falls m das Produkt $m = pq$ zweier Primzahlen mit $2 < p < q$ ist.

Hinweis: Zeigen Sie, dass die Gleichung $x^2 \equiv_p d$ für jedes $d \in \mathbb{Z}_p^*$ entweder 0 oder 2 Lösungen in \mathbb{Z}_p^* und für jedes $d \in \mathbb{Z}_m^*$ entweder 0 oder 4 Lösungen in \mathbb{Z}_m^* hat.