Übungsblatt 1

Aufgabe 1 ***mündlich***

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

Aufgabe 2 ***mündlich***

Berechnen Sie:

(a) 2602 mod 81,

(b) (-2602) mod 81,

(c) 81 mod 2606 und

(d) (-81) mod 2606.

Aufgabe 3 ***mündlich***

Bestimmen Sie alle involutorischen Schlüssel k (d. h. E_k ist involutorisch) der additiven Chiffre über einem Alphabet mit $m = 26$ Zeichen.

Aufgabe 4 ***mündlich***

Bestimmen Sie die Schlüsselzahl der affinen Chiffre für die Modulwerte $m = 30, 100$ und 1225.

Aufgabe 5 ***mündlich***

(a) Sei $k = (b, c)$ ein Schlüssel der affinen Chiffre mit m Zeichen. 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 der affinen Chiffre mit $m = 35$ Zeichen.

(c) Wie viele involutorische Schlüssel besitzt die affine Chiffre mit m Zeichen, falls $m = pq$ das Produkt zweier Primzahlen p und q 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.