Übungen zur Kryptologie 1 Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 1

Aufgabe 1

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

Aufgabe 2

Berechnen Sie:

a) 2602 mod 81,

b) (-2602) mod 81,

c) 81 mod 2606 und

d) (-81) mod 2606.

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 $b^2 \equiv_m 1$ und $c(b+1) \equiv_m 0$ gilt.

b) Bestimmen Sie alle involutorischen Schlüssel in der affinen Chiffre mit dem Modul $m = 35$.

c) Seien p, q Primzahlen mit $2 < q < q$ und sei $m = pq$.

   (a) Zeigen Sie, dass für jedes $d \in \mathbb{Z}_p^*$ die Gleichung $x^2 \equiv_p d$ entweder 0 oder 2 Lösungen hat.

   (b) Zeigen Sie, dass für jedes $d \in \mathbb{Z}_m^*$ die Gleichung $x^2 \equiv_m d$ entweder 0 oder 4 Lösungen hat.

   (c) Wie viele involutorische Schlüssel existieren in der affinen Chiffre mit einem Alphabet m Zeichen ?