Christian Nelius

5. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 13.5.2011, bis 9.15 Uhr

Gruppen 1 und 2 (Mo): Fach Nr. 3 (orangener Schrank bei D1.348)

Gruppen 3 und 4 (Do): Fach Nr. 11 (orangener Schrank bei D1.348)

Internet: http://math-www.uni-paderborn.de/~chris

Schreiben Sie bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel–Nr. und Nr. Ihrer Übungsgruppe. Heften Sie bitte die Seiten zusammen!
Es können **Bonuspunkte** für die Leistungsnachweis–Klausur erworben werden.
Es ist nur Einzelabgabe erlaubt. **Es sind immer Begründungen erforderlich!**

14. Aufgabe: Die Abbildung $f : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$ sei definiert durch

$$f(r) \;=\; 25 - r \quad (r \in \mathcal{R}_{26})\,.$$

a) Beweise unter Benutzung von (1.8), dass f injekjtiv ist. Ist f auch surjektiv? Begründe!

b) Falls f bijektiv ist, bestimme die Umkehrabbildung von f.

c) Die Abbildung $V : \mathfrak{a} \longrightarrow \mathfrak{A}$ sei definiert durch $V = \Omega^{-1} \circ f \circ \omega$. Berechne ausführlich $V(\mathsf{a}), V(\mathsf{m})$ und $V(\mathsf{x})$. Stelle die Wertetabelle von V auf.

d) Verschlüssele mit V das Wort $\mathsf{monoalphabetisch}$. Entschlüssele $\mathsf{PIBKGLTIZKSRV}$. Mit welcher Abbildung wird entschlüsselt? (6)

15. Aufgabe: a) Seien $k, l \in \mathbb{Z}$ und $n \in \mathbb{N}$. Es gelte $k \bmod n \;=\; l \bmod n$. Beweise:

1) Es folgt $(k+m) \bmod n \;=\; (l+m) \bmod n$ für alle $m \in \mathbb{Z}$.

2) Es folgt $(k \cdot m) \bmod n \;=\; (l \cdot m) \bmod n$ für alle $m \in \mathbb{Z}$.

b) Von einer additiven Chiffre V_k $(k \in \mathcal{R}_{26})$ wird $V_k(\mathsf{f}) = \mathsf{R}$ herausgefunden. Läßt sich daraus k berechnen? Was bedeutet dies für die Verschlüsselung? (4)

16. Aufgabe: a) Berechne für jedes $k \in \mathbb{Z}$ die Bildwerte $\mu_k(0)$ und $\mu_k(13)$.

b) Stelle die Wertetabellen für μ_7 und μ_{12} auf.
Welche der Abbildungen ist bijektiv und welche nicht? Begründe an Hand der Wertetabellen!

c) Seien $k, l \in \mathbb{Z}$. Beweise: $\mu_k = \mu_l \iff k \bmod 26 \;=\; l \bmod 26$.

Hinweis zu c): Es sind zwei Beweisrichtungen erforderlich! (6)

Denke an die Punktetabelle!