

6. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 20.5.2011, 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!**

17. Aufgabe: a) Stelle für die Schlüsselwortchiffre mit dem Schlüssel

$\{s, \text{HAEUFIGKEITSANALYSE}\}$

die Wertetabelle auf und verschlüssele damit das Wort "Schlüsselwortchiffre".

b) Es sei $\mathcal{K}$ ein Klartextalphabet mit 29 Buchstaben und $\mathcal{G}$ ein Geheimtextalphabet mit 35 Buchstaben. Bestimme die Anzahl der monoalphabetischen Verschlüsselungen von $\mathcal{K}$ durch $\mathcal{G}$. Eine Formel genügt als Ergebnis! (4)

18. Aufgabe: Sei $k \in \mathcal{R}_{26}$ beliebig mit $\text{ggT}(k, 26) = 1$. Ferner sei M_k die zugehörige multiplikative Chiffre.

a) Berechne $M_k(a)$ und $M_k(n)$.

b) Es gelte $M_k(g) = Q$. Bestimme daraus k (aber nicht mit Hilfe von Wertetabellen!). Gibt es nur eine Lösung?

c) Kann es ein k geben, für das $M_k(c) = X$ gilt? Begründe deine Antwort. Auch hier darf nicht mit Wertetabellen gearbeitet werden! (5)

Fortsetzung nächste Seite!

19. Aufgabe: Der folgende Geheimtext ist durch eine affine Chiffre $A_{k,l}$ entstanden. Ziel der Aufgabe ist es, die Zahlen k und l zu bestimmen und den Geheimtext zu entschlüsseln.

GIRGVIGDAEUGRZGETLGIHAHGIDORUZIGGIRGRBELGRZEA
AEUGRZIGERZGTGRZEAASBCGIUGRXIHEHGTRAHNGTAHD

Führe dazu die folgenden Schritte aus:

- a) Versuche $A_{k,l}(e)$ und $A_{k,l}(n)$ durch eine Häufigkeitsanalyse zu bestimmen (e kommt wahrscheinlich im Klartext am häufigsten und n am zweithäufigsten vor).
- b) Berechne mit den Ergebnissen aus a) $\eta_{k,l}(4)$ und $\eta_{k,l}(13)$ und versuche Zahlen $k, l \in \mathcal{R}_{26}$ zu finden, die dafür passen könnten. Letzteres läßt sich rechnerisch durchführen!
- c) Stelle für die in b) gefundenen Werte von k und l die Wertetabelle für $A_{k,l}$ auf.
- d) Entschlüssele den Geheimtext und schreibe ihn lesbar auf. (7)

Denke an die Punktetabelle!