Christian Nelius

1. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag, 15.4.2011, 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!**

1. Aufgabe: a) Der folgende Geheimtext ist mit einer Skytale verschlüsselt worden. Entschlüssele ihn und begründe kurz deine Vorgehensweise (der Streifen ist im folgenden waagerecht geschrieben):

DRSIRTRIITESSEINEAHVCNCEANROHIHRLEGLLHTSTRELUREK

ETHUEENYNAENSNMTSTIDSAIAPEMVECTLANNELHEE

b) Wie groß ist in a) ungefähr der Durchmesser der Skytale, wenn für jeden Buchstaben in der Höhe 1.5 cm benötigt werden? (4)

2. Aufgabe: Eine **Verschiebechiffre** $V_\Delta : \mathfrak{a} \longrightarrow \mathfrak{A}$ ist ganz analog zu der Caesar–Verschlüsselung definiert: $a \in \mathfrak{a}$ wird durch irgendeinen Buchstaben $\Delta \in \mathfrak{A} = \{A, B, C, \ldots, Z\}$ verschlüsselt, b dann durch den auf Δ folgenden Buchstaben usw. Nach Z kommt dann A usw., bis alle Buchstaben des Alphabets aufgebraucht sind (Die Caesar–Verschlüsselung ist also die Verschiebechiffre V_D) .

a) Stelle eine Tabelle für die Verschiebechiffre V_K auf und verschlüssele damit den Text

gallia est omnis divisa in partes tres

Woher stammt dieser Text und was bedeutet er?

b) Der folgende Geheimtext ist mit einer Verschiebechiffre verschlüsselt worden. Entschlüssele den Geheimtext, beschreibe dein Vorgehen, schreibe den Klartext lesbar auf und erfülle die gestellte Aufgabe. Welche Verschiebechiffre ist benutzt worden?

BDWZDIZVIORJMOVPAYDZAMVBZRVIINVBOZXVZNVMQZIDQDYDQDXD

(7)