7. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 27.5.2011, 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

Schreibe bitte auf die erste Seite **gut** leserlich Namen, Vornamen, Matrikel–Nr., die Nr. deiner Übungsgruppe und eine **Tabelle** für die Punkte. Hefte bitte die Seiten zusammen!
Es können **Bonuspunkte** für die Leistungsnachweis–Klausur erworben werden.
Es ist nur Einzelabgabe erlaubt. **Es sind immer Begründungen erforderlich!**

20. Aufgabe: Der folgende Geheimtext ist durch eine monoalphabetische Verschlüsselung entstanden

I E Z I F Y A Y X F Y Z I K F E H H V I N S C Z M K C I Z E U T R E I B U K F Q E I V E

G I V M B U I E Z I A Y Z Y M B X F M L I T E U K F I R I V U K F B S I U U I B S Z G

a) Stelle eine Tabelle der Häufigkeiten der Geheimtextbuchstaben auf.

b) Versuche, den Geheimtext zu entschlüsseln. Das Vorgehen soll kurz beschrieben und begründet werden. Schreibe den Klartext lesbar auf. (8)

21. Aufgabe: a) Stelle für eine homophone Chiffre von $\mathfrak{a}$ durch das Geheimtextalphabet $\{333, 334, 335, \ldots, 481, 482\}$ eine Tabelle auf, in der für jeden Buchstaben $\gamma \in \mathfrak{a}$ die **Anzahl** der Buchstaben des Geheimtextalphabetes angegeben ist, die γ verschlüsseln sollen.

b) Auf wieviele Arten läßt sich das Wort "himalaya" mit der homophonen Chiffre aus (6.2) verschlüsseln? Dabei soll die Verschlüsselung des Wortes aus lauter verschiedenen Geheimtextbuchstaben bestehen. (4)

22. Aufgabe: a) Sei V eine Vigenère–Chiffre mit dem Schlüsselwort "VIGENERE". Der 167–te Buchstabe des zu verschlüsselnden Klartextes sei "h". Bestimme die Verschlüsselung von h durch V.

b) Sei V' eine Vigenère–Chiffre mit einem Schlüsselwort aus 11 Buchstaben. Der 183–te Buchstabe des zu verschlüsselnden Klartextes sei "j", der durch V' auf C verschlüsselt wird. Läßt sich aus diesen Angaben ein Buchstabe des Schlüsselwortes bestimmen? Wenn ja, welcher? Begründe! (3)