8. Aufgabenblatt

KRYPTOGRAPHIE (für GHRG) (SS 2011)

Abgabe: Freitag 3.6.2011, 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!**

23. Aufgabe: Der folgende Geheimtext *GT* ist durch eine Vigenère–Chiffre entstanden

F	Z	M	F	Q	O	O	K	J	H	Y	Z	S	P	Y	J	H	V	F	L	X	G	X	R
X	G	X	V	W	A	Y	E	X	Q	B	N	F	G	F	V	W	B	Y	E	R	I	M	J
S	W	W	Y	Y	O	F	C	J	W	H	U	F	G	U	S	H	P	L	Z	S	U	N	U
J	B	G	V	S	G	W	Y	J	B	C	E	I	W	Y	Y	T	S	B	E	N	Q	B	K
F	Z	F	V	N	B	C	D	X	Q	B	I	J	W	V	V	S	Z	Y	J	J	B	O	V
G	H	M	Z	H	V	Y	Z	S	J	Y	I	S	I	Y	E	K	H	C	X	B	S	M	V
S	B	C	T	M	H	U	C	Q	S	C	E	N	B	L	V	H	V	H	L	S	U	M	J
F	Q	B	V	S	G	I	C	Q	R	Y	I	R	S	H	J	H	V	M	Z	H	V	G	L
J	V	Y	D	F	Q	B	V	S	G	I	E	I	S	L	E	F	I	W	Y	I	S	L	N
J	W	M	Y	J	W	N	C	J	V	L	V	S	A	O	J	X	A	U	E	R	W	N	M
J	F	A	E	Z	S	A	V	S	V	I	V	W	S	H	N	G	I	M	T	M			

a) Berechne den Koinzidenzindex von *GT*. Was läßt sich daraus über die Art der Verschlüsselung folgern?

b) Berechne mit dem Friedman–Test (7.13) die ungefähre Länge des Schlüsselwortes für die Vigenère–Chiffre.

c) Bestimme mit dem Kasiski–Test die Schlüsselwort–Länge. Hierfür sind möglichst viele (mindestens aber 5) gleiche Buchstabenreihen aus mindestens 3 Buchstaben zu finden, die alle unterschiedliche Abstände haben.

d) Bestimme das Schlüsselwort. Gib dabei eine kurze Beschreibung und Begründung deines Vorgehens.

Hinweis: Um zu prüfen, ob ein Schlüsselwort richtig sein kann, genügt es meistens, damit erst einmal nur einen kleinen Teil des Geheimtextes zu entschlüsseln.

e) Entschlüssele den Geheimtext und schreibe ihn lesbar auf. (14)