Übungen zur Diskreten Mathematik (Lehramt GM/So)

WiSe 06/07 W. Huang und H.-J. Samaga **Blatt 6**

A: Präsenzaufgaben und Verständnisfragen

23. Man entschlüssele den berühmten Ausspruch von Cäsar: SBKF SFAF SFZF .

24. Der monoalphabetisch verschlüsselte englische Satz A BC B CBD trifft nicht auf die Mehrheit in dieser Übungsgruppe zu. Wie hätte er statt dessen bei gleicher Verschlüsselung heißen können?

25. Ergänze folgende Tabelle eines unknackbaren Codes: (Hinweis: Modulo 26–Rechnung)

Schlüsselwort	BFUM	BFUM	ALTP		
Klartext	BUCH	CODE		GELD	
Geheimtext			CZWT	CZWT	BANA

26. Mit dem öffentlichen Schlüssel ($n = 31,\ e = 13$) wird eine Nachricht m in den Geheimtext $c = me \bmod n$ verwandelt. Gesucht ist der Geheimtext zur Nachricht $m = 10$ und die Nachricht zum Geheimtext $c = 11$.

B: Übungsaufgaben

17. In Aufgabe **A 21** (Blatt 5) wurden beim linearen $(7, 4)$–Code aus der Vorlesung Fehler mit Hilfe von Matrizenrechnung entdeckt. Wie lautet die Matrix bei gleicher Vorgehensweise im Fall des Linearcodes $\{000, 111\}$? Ist dieser Code perfekt? (Jeweils mit Begründung)

18. In dem monoalphabetisch verschlüsselten Text im Beutelspacher auf Seite 132 (Aufgabe 5) geht es um eine historische Gestalt; hier ein kurzer Ausschnitt:

gmxi jca ecaxc dvfcav gqaqxvd wjclwxi scpaq xl qlinxdupqa iqmcliqldupcmv. qxlqa xpaqa clpcqliqa qadcll oql rncl, qnxdcgqvp oxq qadvq hbl qlinclo wf qaebaoql flo ocofaup qxlql cfmdvclo oqa qlinxdupql ycvpbnxyql cfdwfnbqdql exv oqe wxqn, ecaxc wfa ybqlxixl hbl qlinclo wf yabqlql.

Man decodiere diesen Ausschnitt (Hinweis: Das Wort gmxi steht für eine Jahreszahl).

19. Wie lautet die folgende mit einer Skytala verschlüsselte Nachricht (siehe auch Beutelspacher, Seite 133):

I S A D T P I H E H N N C S D I R O O I L T A I H T A E A S
N F E Z C S W E S S N I S F I U K T U J S E S T C R C K E !

20. Zur Eulerschen φ–Funktion: $\mathbb{N} \to \mathbb{N},\ \varphi(n) := |\{1 \le k \le n \mid \mathrm{ggT}(k, n) = 1\}|$:

a) Gesucht sind vier verschiedene $n \in \mathbb{N}$ mit $\varphi(n) = 6$.

b) Gesucht sind $\varphi(2048)$ und $\varphi(7^4)$.

b) Gesucht sind Primzahlen p und q mit $pq = 14803$ und $\varphi(pq) = 14560$.

Abgabe von drei der vier Übungsaufgaben : Dienstag, 5. Dezember 06, in den Übungen. Welche der Aufgaben behandelt werden sollen, wird in den Übungen bekannt gegeben, bei Abgabe aller Aufgaben gibt es Extrapunkte.