

## Übungsblatt 3

### Aufgabe 11

*mündlich*

Ver- und entschlüsseln Sie den Klartext STEFFENFREUND mit dem Schlüssel FCK unter einem

- (a) Vigenère-System,
- (b) Beaufort-System,
- (c) Autokey-System (mit Klartext- und mit Kryptotextschlüsselstrom).

### Aufgabe 12

*mündlich*

Überlegen Sie, wie man durch »elementare Zeilenoperationen« die Inverse einer Matrix  $A \in \mathbb{Z}_m^{l \times l}$  effizient berechnen kann und wenden Sie Ihre Methode auf die  $4 \times 4$ -Schlüsselmatrix aus der Vorlesung an.

### Aufgabe 13

*mündlich*

Es liege ein durch ein Autokey-System mit Klartextschlüsselstrom erzeugter Kryptotext  $y$  vor. Führen Sie die Analyse dieser Chiffre auf die Analyse der Vigenère-Chiffre zurück (die Schlüssellänge  $d$  kann als bekannt vorausgesetzt werden).

*Hinweis:* Entschlüsseln Sie  $y$  mit einem beliebigen Schlüsselwort (z.B.  $k = A \dots A$ ) und betrachten Sie den resultierenden »Klartext«.

### Aufgabe 14

**10 Punkte**

Sei  $A = (a_{ij}) \in \mathbb{Z}_m^{l \times l}$  eine  $l \times l$ -Matrix,  $l \geq 1$ . Zeigen Sie, dass die Abbildung  $f : \mathbb{Z}_m^l \rightarrow \mathbb{Z}_m^l$  mit

$$f(x_1, \dots, x_l) = (y_1, \dots, y_l) \text{ mit } y_i = x_1 a_{1i} + \dots + x_l a_{li} \pmod{m}$$

genau dann injektiv ist, wenn  $\text{ggT}(\det(A), m) = 1$  ist.

*Hinweis:* Betrachten Sie die zu  $A$  adjungierte Matrix  $\tilde{A} = (\tilde{a}_{ij})$ , wobei

$$\tilde{a}_{ij} = (-1)^{i+j} \det(A_{ji})$$

ist, und leiten Sie die Gleichung

$$\tilde{A} \cdot A = \det(A) \cdot E$$

her ( $E$  ist die Einheitsmatrix und  $A_{ij}$  ist die durch Streichen der  $i$ -ten Zeile und  $j$ -ten Spalte aus  $A$  hervorgehende Matrix.)