Übungen zur Kryptologie 1 Wintersemester 2003-2004

Johannes Köbler/Lorenz Weizsäcker

Übungsblatt 3

Aufgabe 11

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 (schriftlich, 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 $f : \mathbb{Z}_m^l \to \mathbb{Z}_m^l$ mit

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

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

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

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

ist, und leiten Sie die Gleichung

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

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

Aufgabe 13

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 4×4-Schlüsselmatrix aus der Vorlesung an.

Aufgabe 14

Es liege ein durch ein Autokey-System mit Klartextschlüsselstrom erzeugter Kryptotext y vor. Führen Sie die Analyse dieser Chiffre unter der Annahme, dass die Schlüssellänge d bekannt ist, auf die Analyse der Vigenère-Chiffre zurück.

Hinweis: Entschlüsseln Sie y mit einem beliebigen Schlüsselwort (z.B. $k = A \ldots A$) und betrachten Sie den resultierenden „Klartext“.