Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler

Sommersemester 2000
10. Mai 2000

Übungen zur Kryptologie

3. Übung

Abgabe am 24. Mai 2000

Aufgabe 10 (*schriftlich zu bearbeiten,* 4 Punkte)
Bei einer affinen Chiffre wurde durch Häufigkeitsanalyse festgestellt, dass E auf h und N auf v abgebildet wurde. Wie lautet der Schlüssel?
Welche Schlüssel kommen in Frage, wenn X auf s und Z auf e abgebildet wird?

Aufgabe 11 (*schriftlich zu bearbeiten,* 5 Punkte)
Bestimmen Sie die Anzahl der Lösungen $x \in \{0, \dots, m-1\}$ der Kongruenzgleichung

$$ax \equiv_m b$$

in Abhängigkeit von $\mathrm{ggT}(m, a)$ und b. Betrachten Sie zunächst den Fall $b = 0$.

Aufgabe 12 (*schriftlich zu bearbeiten,* 9 Punkte)
Verschlüsseln Sie den Text

KLARTEXT

mittels einer

a) Polybios-Chiffre (mit dem Schlüssel aus der Vorlesung),
b) Freimaurer-Chiffre (mit dem Schlüssel aus der Vorlesung),
c) additiven Chiffre (Schlüssel 13),
d) affinen Chiffre (Schlüssel (25,2)),
e) Spionage-Chiffre (Schlüsselwort INGEFAHR, Spalten und Zeilennummerierung wie in der Vorlesung),
f) homophonen Chiffre (wie in der Vorlesung),
g) Playfair-Chiffre (Schlüssel aus der Vorlesung),
h) Delastelle-Chiffre (Schlüssel aus der Vorlesung),
i) Hill-Chiffre (4×4 Schlüsselmatrix aus der Vorlesung).

Aufgabe 13 (*schriftlich zu bearbeiten,* 2 Punkte)
Ein Kryptotext sei mittels einer homophonen monographischen und monopartiten Chiffre erstellt worden. Eine Häufigkeitsanalyse zeigt, dass im Kryptotext alle Kryptotextzeichen mit (etwa) derselben Häufigkeit vorkommen. Überlegen Sie, wie der Kryptotext mittels Bigramm-Analyse geknackt werden kann.

Aufgabe 14 (*schriftlich zu bearbeiten*, 8 Punkte)
Sei $M \in \mathbb{Z}_m^{l \times l}$. Sei $\mathbf{x} = (x_1, \ldots, x_l)$. Zeigen Sie, die Funktion $E_M : \mathbb{Z}_m^l \to \mathbb{Z}_m^l$ mit

$$E_M(\mathbf{x}) = M\mathbf{x}^T$$

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

a) Es gilt $\det(AB)=\det(A)\cdot\det(B)$.

b) Für die zu A adjungierte Matrix A_{adj} gilt

$$A \cdot A_{\mathrm{adj}} = \det(A) \cdot I\,. \quad (*)$$

Dabei sei I die Einheitsmatrix und $A_{\mathrm{adj}} = (a'_{ij})_{1 \leq i,j \leq l}$ mit

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

wobei $A_{\overline{ji}}$ aus A durch Streichen der j-ten Zeile und der i-ten Spalte hervorgeht.

Begründen Sie auch, dass die Gleichung $(*)$ gilt!