Übungsblatt 3

Aufgabe 13 ***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 14 ***mündlich***

(a) Durch eine Hill-Chiffre mit unbekanntem Schlüssel wird der Klartext `CONSPIRACIES` zum Kryptotext *RPETVTZADECM* abgebildet. Bestimmen Sie die minimale Blocklänge l und eine $(l \times l)$-Schlüsselmatrix, die diese Chiffrierfunktion realisiert.

(b) Geben Sie eine Hill-Schlüsselmatrix der Dimension $l \leq 4$ an, die `CONVERSATION` zu *HIARRTNUYTUS* verschlüsselt.

(c) Bei kleiner Blocklänge l kann die Hill-Chiffre durch eine Häufigkeitsanalyse gebrochen werden. Im Fall $l = 2$ unterteilt man beispielsweise den Kryptotext in Bigrammblöcke und nimmt an, dass im Kryptotext häufig vorkommende Bigramme aus häufigen Bigrammen der Klartextsprache entstanden sind. Verwenden Sie diesen Ansatz, um den zu dem Kryptotext

LM QE TX YE AG TX CT UI EW NC TX LZ EW UA IS PZ YV AP EW LM GQ WY AX
FT CJ MS QC AD AG TX LM DX NX SN PJ QS YV AP RI QS MH NO CV AX FV

gehörigen englischen Klartext zu bestimmen. (*Hinweis:* Das Urbild des häufigsten Kryptotext-Bigramms *TX* ist `IN`.)

Aufgabe 15 ***mündlich***

(a) Wie wirken sich das Addieren einer Zeile auf eine andere, der Tausch zweier Zeilen und die Multiplikation einer Zeile mit $r \in \mathbb{Z}_m$ auf die Determinante einer Matrix $A \in \mathbb{Z}_m^{l \times l}$ aus?

(b) Finden Sie mittels a) eine effiziente Methode zur Berechnung der Determinante $\det(A)$.

(c) Erweitern Sie die Methode aus b), sodass sie auch das Inverse A^{-1} effizient berechnet und wenden Sie sie (inkl. Determinante) auf die (4×4)-Schlüsselmatrix aus der Vorlesung an.

Aufgabe 16 ***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 $f(x) = xA$ 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.)