Übungsblatt 3

Abgabe der schriftlichen Lösungen am 16. 11. 2017 bis 13.10 Uhr

Aufgabe 13 ***mündlich***

Bestimmen Sie für $m = 6, 8$ und 26 die Anzahl der invertierbaren (2×2)-Matrizen über $\mathbb{Z}_m$.

Hinweis: Benutzen Sie Aufgabe 17 und den Chinesischen Restsatz.

Aufgabe 14 ***mündlich***

(a) Zeigen Sie, dass für jede selbstinverse Matrix A über $\mathbb{Z}_{26}$ gilt: $\det(A) \equiv_{26} \pm 1$.

(b) Bestimmen Sie die Anzahl der selbstinversen (2×2)-Matrizen über $\mathbb{Z}_{26}$.

Hinweis: Benutzen Sie den Chinesischen Restesatz.

Aufgabe 15 ***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 16 ***mündlich, rechenintensiv***

(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 17 Sei p prim. ***10 Punkte***

(a) Zeigen Sie, dass genau $(p^2 - 1)(p^2 - p)$ invertierbare (2×2)-Matrizen über $\mathbb{Z}_p$ existieren.

(b) Bestimmen Sie die Anzahl aller invertierbaren $(k \times k)$-Matrizen über $\mathbb{Z}_p$.

Hinweis: Benutzen Sie, dass eine $(k \times k)$-Matrix über $\mathbb{Z}_p$, p prim, genau dann invertierbar ist, wenn die Zeilen der Matrix linear unabhängige Vektoren (über $\mathbb{Z}_p$) sind.