

Aufgabe 5: (14 Punkte)

Betrachten Sie die folgende, von *Lester S. Hill* im Jahr 1929 erfundene Blockchiffre über dem Alphabet $A = \{\mathbf{a}, \mathbf{b}, \dots, \mathbf{z}, \mathbf{\ddot{a}}, \mathbf{\ddot{o}}, \mathbf{\ddot{u}}\}$ bzw. $A = \{0, 1, \dots, 25, 26, 27, 28\}$.

- Schlüssel: 2×2 -Matrix $K = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$ mit $k_{ij} \in A$ für $i, j \in \{1, 2\}$
- Verschlüsseln: Stelle den Klartext als Zahlenfolge $P = (P_1, P_2, \dots, P_{2m})$ mit $P_i \in \{0, 1, \dots, 28\}$ dar und unterteile P in Blöcke (P_i, P_{i+1}) der Länge 2 für $i = 1, 3, \dots, 2m-1$. Verschlüssele jeden Block (P_i, P_{i+1}) zum Geheimtext (C_i, C_{i+1}) durch die Matrixmultiplikation

$$\begin{pmatrix} C_i \\ C_{i+1} \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \cdot \begin{pmatrix} P_i \\ P_{i+1} \end{pmatrix},$$

wobei alle grundlegenden Rechenoperationen modulo $|A| = 29$ durchgeführt werden.

- (a) Was ist bei der Wahl der Schlüsselmatrix zu beachten?
Wie sieht die zugehörige Entschlüsselungsfunktion aus?
- (b) Entschlüsseln Sie den Geheimtext **RKNT**, der mit der Schlüsselmatrix $K = \begin{pmatrix} \mathbf{D} & \mathbf{O} \\ \mathbf{R} & \mathbf{T} \end{pmatrix}$ verschlüsselt wurde.
- (c) Angenommen, Sie kennen folgende Hill-Verschlüsselungen:

$$\begin{aligned} E\left(\begin{pmatrix} \mathbf{m} \\ \mathbf{d} \end{pmatrix}, K\right) &= \begin{pmatrix} \mathbf{P} \\ \mathbf{G} \end{pmatrix} \\ E\left(\begin{pmatrix} \mathbf{b} \\ \mathbf{i} \end{pmatrix}, K\right) &= \begin{pmatrix} \mathbf{W} \\ \mathbf{H} \end{pmatrix} \end{aligned}$$

Wie lautet der Schlüssel K ?

- (d) Leiten sie aus der vorigen Teilaufgabe einen allgemeinen Known-Plaintext-Angriff auf die Hill-Chiffre ab, mit dem die Schlüsselmatrix geknackt werden kann. Unter welcher Voraussetzung funktioniert der Angriff?
- (e) In wie weit erhöht sich die Sicherheit des Verfahrens, wenn eine $n \times n$ -Schlüsselmatrix mit $n \geq 3$ verwendet wird?

Aufgabe 6: (6 Punkte)

- (a) Konstruieren Sie ein LFSR der Länge 4, das einen Nicht-Null-Zustand in den Null-Zustand überführt.
(Hinweis: „Nullzustand“ bedeutet, dass alle Registerzellen den Wert 0 haben.)
- (b) Die Ausgabefolge 0000100011 wurde von einem LFSR der Länge 5 erzeugt. Welches Schieberegister wurde verwendet? Geben Sie die Rückkopplungsfunktion an.