8.8 Die HILL-Chiffre

Beschreibung

Das **Alphabet** ist $\Sigma = \mathbb{Z}/n\mathbb{Z}$ mit der Struktur als endlicher Ring.

Der **Schlüsselraum** ist $K = GL_l(\mathbb{Z}/n\mathbb{Z})$, die multiplikative Gruppe der invertierbaren Matrizen. Die Größe des Schlüsselraums wird in Abschnitt 8.9 abgeschätzt.

Verschlüsselt wird blockweise, wobei l die Blocklänge ist: Für $k \in GL_l(\mathbb{Z}/n\mathbb{Z})$ und $(a_1, \ldots, a_l) \in (\mathbb{Z}/n\mathbb{Z})^l$ ist

$$\begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix} = f_k(a_1, \ldots, a_l) = k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix}$$

oder in ausgeschriebener Form

$$c_i = \sum_{j=1}^{l} k_{ij} a_j \quad \text{für } i = 1, \ldots, l.$$

Entschlüsselt wird mit der inversen Matrix:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = k^{-1} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix}.$$

Verwandte Chiffren

Spezialfall: Wird k als Permutationsmatrix P_σ zur Permutation $\sigma \in \mathcal{S}_l$ gewählt, so ist die Verschlüsselungsfunktion f_k die Blocktransposition zu σ.

Verallgemeinerung: Die affine Chiffre. Hier wird ein Schlüssel

$$(k, b) \in GL_l(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^l$$

gewählt; verschlüsselt wird nach der Formel

$$c = ka + b.$$

Wählt man hier k als die Einheitsmatrix, so erhält man als Spezialfall wiederum die BELASO-Chiffre mit Schlüssel b.

Anmerkung: Bei der von HILL vorgeschlagenen Original-Chiffre wird vor Anwendung der linearen Abbildung zunächst noch das Alphabet permutiert, d. h., die Zuordnung der Buchstaben zu den Zahlen $0, \ldots, 25$ wird als Teil des Schlüssels angesehen.

Beispiel

Zur Illustration ein „Spielzeug-Beispiel“ mit ganz unvernünftig kleiner Dimension $l = 2$ und

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Dann ist $\operatorname{Det} k = 77 - 24 = 53 \equiv 1 \bmod 26$ und

$$k^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

Zur Umrechnung von Zahlen in Buchstaben ist es nützlich, die Tabelle

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

zur Hand zu haben. Damit wird der Klartext `Herr` $= (7, 4, 17, 17)$ verschlüsselt zu

$$\begin{aligned} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} &= \begin{pmatrix} 77 + 32 \\ 21 + 28 \end{pmatrix} = \begin{pmatrix} 109 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix}, \\ \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 17 \end{pmatrix} &= \begin{pmatrix} 187 + 136 \\ 51 + 119 \end{pmatrix} = \begin{pmatrix} 323 \\ 170 \end{pmatrix} = \begin{pmatrix} 11 \\ 14 \end{pmatrix}, \end{aligned}$$

also $f_k(\texttt{Herr}) = (5, 23, 11, 14) = \texttt{FXLO}$.

Zur Probe die Entschlüsselung:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} = \begin{pmatrix} 35 + 414 & 77 + 252 \\ 115 + 253 & 253 + 154 \end{pmatrix} = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Bewertung

\+ Wesentlich stärker als die Blocktransposition und die Belaso-Chiffre.

\+ Die Geheimtexte sind sehr gut gleichverteilt; ein Angriff mit nichts als Geheimtext findet keine Anhaltspunkte.

\− Sehr anfällig für einen Angriff mit bekanntem Klartext, siehe Abschnitt 8.10.