Marko Roczen und Helmut Wolter
unter Mitarbeit von
Wilfred Pohl, Dorin Popescu, Radu Laza

Aufgabensammlung[1]
Lineare Algebra individuell ◁ zur Fundstelle

Aufgabe 3/3/240 (S: Varianten)
Hill-Ciphern (3)

Index: Vektorraum, lineare Abbildung, Hill-Ciphern, Entschlüsselung durch lineare Fortsetzung, lineare Fortsetzung

Stoffeinheiten: 3/3/29 Beispiel: Entschlüsselung von Hill - Ciphern

Eine Nachricht wird in der folgenden Weise verschlüsselt, indem zunächst Buchstaben auf Elemente des Primkörpers $\mathbb{F}_{29}$ abgebildet werden.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z	-	,	
15	16	17	18	19	20	21	22	23	24	25	26	27	28

Die entstandenen Ziffern werden als Folge von Zahlenpaaren angeordnet (wobei ggf. am Ende der Nachricht ein Leerzeichen einzufügen ist, damit eine gerade Anzahl von Buchstaben entsteht).
Nun bezeichne A eine reguläre Matrix aus $\mathrm{M}(2;\mathbb{F}_{29})$; die zugehörige lineare Abbildung $\mathbb{F}_{29}^2 \to \mathbb{F}_{29}^2$ der Standardräume bildet die Paare der Folge auf neue Paare ab.
Als verschlüsselte Nachricht bezeichnen wir denjenigen Text, der der Folge der Bilder der Zahlenpaare entspricht.
HUGO hat eine Nachricht unter Verwendung der Matrix $A \in \mathrm{M}(2,\mathbb{F}_{29})$ nach obiger Methode verschlüsselt; diese lautet nun

„PZGFN ZVRQJM“.

Wir nehmen an, dass HUGO in der Nachricht eine gerade Anzahl von Zeichen verwendet und der Brief mit dem Vornamen HUGO endet.
Entschlüsseln Sie die Nachricht.

Lösung. Zunächst stellen wir die Zuordnung der Buchstaben zu den Elementen von $\mathbb{F}_{29}$ her und erhalten die folgende Liste von Paaren

$$(15,25),(6,5),(13,28),(25,21),(17,16),(9,12).$$

Wir haben die Matrix A zu finden. Nun sind „HU “ und „GO “ die letzten beiden Buchstabenpaare der Nachricht. Offensichtlich entsprechen diese gerade den Zahlenpaaren

[1] Ver. 0.51 (Juli 2004), Institut für Mathematik an der Mathematisch-Naturwissenschaftlichen Fakultät II der Humboldt-Universität zu Berlin, 2004 (Preprint; 2004-17), ISSN 1439-9679
Diese Aufgabensammlung entstand mit teilweiser Förderung durch das Bundesministerium für Bildung und Forschung unter dem Kennzeichen 01NM075D; die Verantwortung für den Inhalt liegt bei den Autoren.
Ähnliche Aufgaben finden Sie im gleichnamigen Internetprojekt Lineare Algebra individuell; als registrierter Nutzer können Sie dort online Aufgaben erzeugen und Lehrstoff nach eigenem Wunsch zusammenstellen lassen.

$w_1 = (7, -9)$ und $w_2 = (6, 14)$. Durch Multiplikation ihrer Transponierten mit der Matrix A erhalten wir die letzten zwei Paare der obigen Liste, d.h. $u_1 = (-12, -13)$ $u_2 = (9, 12)$. Es folgt $A \cdot W = U$ mit

$$U = \begin{pmatrix} -12 & 9 \\ -13 & 12 \end{pmatrix}, \quad W = \begin{pmatrix} 7 & 6 \\ -9 & 14 \end{pmatrix}.$$

Daraus ergibt sich

$$A = U \cdot W^{-1} = \begin{pmatrix} 0 & 11 \\ 6 & -10 \end{pmatrix}.$$

Durch Multiplikation der Transponierten der Paare u mit der Matrix

$$A^{-1} = \begin{pmatrix} -6 & 5 \\ 8 & 0 \end{pmatrix},$$

d.h. durch ${}^t u \mapsto A^{-1} \cdot {}^t u$ erhalten wir die gesuchten Urbilder; das erste entsteht beispielsweise durch

$$\begin{pmatrix} 15 \\ 25 \end{pmatrix} \mapsto A^{-1} \cdot \begin{pmatrix} 15 \\ 25 \end{pmatrix} = \begin{pmatrix} 6 \\ 4 \end{pmatrix}.$$

Die Resultate werden wiederum als Liste von Paaren aus $\mathbb{F}_{29}^2$ angeordnet; es ergibt sich

$$(6, 4), (18, 19), (4, 17), (13, 26), (7, 20), (6, 14).$$

Wir stellen gemäß der Tabelle die Zuordnung zu den Buchstaben her und erhalten die unverschlüsselte Nachricht

„GESTERN-HUGO“.