Codierung und Verschlüsselung (5)

Ein weiteres Beispiel für eine *polyalphabetische* Verschlüsselung ist die Codierung mit Hilfe spezieller Matrizen, wie wir sie z.B. bei den geometrischen Abbildungen kennen gelernt haben. Dazu müssen wir zunächst einmal Buchstaben natürlichen Zahlen zuordnen. Wir begnügen uns mit kleinen Buchstaben.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	ä	ö	ü	ß	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

Wir haben also einen Zeichensatz von 31 Zeichen, weil wir auch die Leerstelle benötigen, wenn unser Text nicht aus einer geraden Anzahl von Zeichen besteht.

Wir nehmen als Codiermatrix: $\mathbf{C} := \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$

Diese Matrix ordnet einem Zahlenpaar $\begin{pmatrix} x \\ y \end{pmatrix}$ ein neues Zahlenpaar $\begin{pmatrix} x' \\ y' \end{pmatrix}$ zu und wir müssen unseren zu verschlüsselnden Text nur in Form von solchen Zahlenpaaren schreiben.

.....

Text: **aoc aahqodpßruaobourßazrak**dasleichtesteigtdasschwerefällt

Oh, der erste Teil des Textes ist im Original wohl verloren gegangen, während dem Codierer offensichtlich auf halber Strecke „die Luft ausgegangen“ ist. - Führe seine Arbeit zu Ende (2 Bildpaare sind schon eingetragen)!

$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$																
	3	18	4	2	19	18	4	6	3	18	2	22	17	5	11	19
	0	11	8	7	4	19	8	19	0	18	7	4	4	26	11	30
	15						36									
	6						16									

Ordne nun den Zahlen der Bildpaare wieder Buchstaben zu (möglicherweise musst du eine Rechnung modulo 31 durchführen) und ergänze den teilweise verschlüsselten Text. - Ist dir verständlich, warum wir bei dieser Methode unbedingt die Leerstelle benötigen?

Codierter Text: **aoc aahqodpßruaobourßazrak**

.....

Nun wollen wir versuchen, den Anfang des Originaltextes wieder herzustellen, schließlich verfügen wir ja über den codierten Text und kennen die Codiermatrix **C**. - Kann man damit eine Decodiermatrix **D** bestimmen? - Wenn ja, doch wie?

$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}$																
$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	0	2	0	7												
	14	30	0	16												

Ergänze den unteren Teil der Tabelle mit den fehlenden Zahlenpaaren und überlege was aus einem Zahlenpaar wird, auf das man zuerst **C**, danach auf das Bildpaar **D** anwenden würde.

.....

Für die Decodiermatrix muß gelten: $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix} \right) \circ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \circ \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$

Begründe, dass sich daraus die folgenden 2 Linearen Gleichungssysteme ergeben:

$$\left\{ \begin{array}{rcl} 5 \cdot a + 2 \cdot b = 1 \\ \wedge\ 2 \cdot a + 1 \cdot b = 0 \end{array} \right\} \qquad \left\{ \begin{array}{rcl} 5 \cdot c + 2 \cdot d = 0 \\ \wedge\ 2 \cdot c + 1 \cdot d = 1 \end{array} \right\}$$

Löse die beiden Gleichungssysteme und bestimme damit die Decodiermatrix **D**. Führe eine Proberechnung durch die Verknüpfung: **D** ∘ **C** durch.

Entschlüssele mit **D** den ersten Teil des Textes (möglicherweise musst du eine Rechnung modulo 31 durchführen - was heißt das eigentlich bei negativen Zahlen?!) und notiere nachfolgend den vollständigen Originaltext.

Originaltext:[1]

Übung (HA): Es sei $\mathbf{C} := \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ und der teilweise schon verschlüsselte Text lautet:

hättnichtderseemanndenhumor**pfbuätoläwmipzvellxßqdoa**

Bestimme den vollständig codierten Text und rekonstruiere den vollständigen Originaltext!

Codierter Text:

Originaltext:

Gegeben Sei die Codiermatrix $\mathbf{C} := \begin{pmatrix} 4 & 2 \\ 2 & 1 \end{pmatrix}$

Verschlüssele damit das Wort: mathematik

Versuche nun das verschlüsselte Wort über eine Decodiermatrix wieder zu entschlüsseln. - Nimm zu der Frage Stellung, ob alle 2×2 - Matrizen zum Codieren geeignet sind. - Begründe deine Meinung.

---

[1] von Gotthold Ephraim **Lessing** (✳ 22.01.1729 Kamenz / Oberlausitz; ✝ 15.02.1781 Braunschweig)