Hill-Chiffre

Musterlösung

André Huber
huberа@bluewin.ch

A1

IUD QUFJIGIQ VIGTXJGID CXQUIGM XZT IUDIP KIJIUPID QFJBZIQQIB.

EIN SICHERES VERFAHREN BASIERT AUF EINEM GEHEIMEN SCHLUESSEL

Chiffre	I	U	D	Q	F	J	G	V	T	X	C	M	Z	P	K	B
Anzahl	13	5	4	6	2	4	4	1	2	3	1	1	2	2	1	2
Klartext	E	I	N	S	C	H	R	V	F	A	B	T	U	M	G	L

A2

a) FAUL $\hat{=}$ 5 0 20 11

$\Rightarrow A = \begin{pmatrix} 5 & 0 \\ 20 & 11 \end{pmatrix}$

G E | H E | I M

6 4 | 7 4 | 8 12

$\Rightarrow \vec{u}_1 = \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \vec{u}_2 = \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \vec{u}_3 = \begin{pmatrix} 8 \\ 12 \end{pmatrix}$

$A \cdot \vec{u}_1 = \begin{pmatrix} 5 & 0 \\ 20 & 11 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 4 \end{pmatrix} = \begin{pmatrix} 30 \\ 164 \end{pmatrix}$ $\Rightarrow \vec{v}_1 = \begin{pmatrix} 30 \\ 164 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$

$A \cdot \vec{u}_2 = \begin{pmatrix} 5 & 0 \\ 20 & 11 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 4 \end{pmatrix} = \begin{pmatrix} 35 \\ 184 \end{pmatrix}$ $\Rightarrow \vec{v}_2 = \begin{pmatrix} 35 \\ 184 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 \\ 2 \end{pmatrix}$

$A \cdot \vec{u}_3 = \begin{pmatrix} 5 & 0 \\ 20 & 11 \end{pmatrix} \cdot \begin{pmatrix} 8 \\ 12 \end{pmatrix} = \begin{pmatrix} 40 \\ 292 \end{pmatrix}$ $\Rightarrow \vec{v}_3 = \begin{pmatrix} 40 \\ 292 \end{pmatrix} \bmod 26 = \begin{pmatrix} 14 \\ 6 \end{pmatrix}$

4 8 | 9 2 | 14 6

E I J C O G

Das Wort GEHEIM wird zu EIJCOG verschlüsselt.

b) Die Matrixmultiplikation wird mit ihrer Inversen rückgängig gemacht, so auch die Verschlüsselung:

$A^{-1} = \frac{1}{55} \cdot \begin{pmatrix} 11 & 0 \\ -20 & 5 \end{pmatrix}$

$A^{-1} \cdot \vec{v}_1 = \frac{1}{55} \cdot \begin{pmatrix} 11 & 0 \\ -20 & 5 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 8 \end{pmatrix} = \frac{1}{55} \cdot \begin{pmatrix} 44 \\ -40 \end{pmatrix} = \begin{pmatrix} \frac{4}{5} \\ -\frac{8}{11} \end{pmatrix}$

PROBLEM: Was haben diese Brüche zu bedeuten?

A3

a) Das folgende kurze Python-Programm erledigt die Aufgabe:

```
n = 26 # Länge des Alphabets
for i in range(n):
    for j in range(n):
        if ((i*j)%n == 1):
            print(i,"*",j,"mod",n,"=",1)
```

b)

i	1	3	5	7	9	11	15	17	19	21	23	25
j	1	9	21	15	3	19	17	23	11	5	17	25

c) Nur zu 26 teilerfremde Zahlen haben eine modulare Inverse.

A4

a) $A^{-1} = 9 \cdot \begin{pmatrix} 11 & 0 \\ -20 & 5 \end{pmatrix} \bmod 26 = \begin{pmatrix} 99 & 0 \\ -180 & 45 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 & 0 \\ 2 & 19 \end{pmatrix}$

c) $\vec{u}_1 = \begin{pmatrix} 21 & 0 \\ 2 & 19 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 8 \end{pmatrix} \bmod 26 = \begin{pmatrix} 84 \\ 160 \end{pmatrix} \bmod 26 = \begin{pmatrix} 6 \\ 4 \end{pmatrix} \begin{matrix} \to G \\ \to E \end{matrix}$

$\vec{u}_2 = \begin{pmatrix} 21 & 0 \\ 2 & 19 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 189 \\ 56 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix} \begin{matrix} \to H \\ \to E \end{matrix}$

$\vec{u}_3 = \begin{pmatrix} 21 & 0 \\ 2 & 19 \end{pmatrix} \cdot \begin{pmatrix} 14 \\ 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 294 \\ 142 \end{pmatrix} \bmod 26 = \begin{pmatrix} 8 \\ 12 \end{pmatrix} \begin{matrix} \to I \\ \to M \end{matrix}$

A5

a) MAMA: $A = \begin{pmatrix} 12 & 0 \\ 12 & 0 \end{pmatrix}$ $\det(A) = 0$ => Matrix nicht invertierbar und daher ungeeignet

TELL: $A = \begin{pmatrix} 19 & 4 \\ 11 & 11 \end{pmatrix}$ $\det(A) = 209 - 44 = 165$

$165 \bmod 26 = 9$

9 und 26 sind teilerfremd

=> Schlüssel geeignet

BAUM: $A = \begin{pmatrix} 1 & 0 \\ 20 & 12 \end{pmatrix}$ $\det(A) = 12$

12 ist gerade, 2 ist also Teiler von 12 und 26

=> Schlüssel ungeeignet

b) Ausprobieren und sicherstellen, dass die beiden Bedingungen erfüllt sind.

A6

a | d) Wenn die Verschlüsselung mind. zweier Bigramme bekannt ist, kann ein lineares Gleichungssystem (LGS) aufgestellt werden, aus dem der Schlüssel errechnet werden kann.

b) E R $\hat{=}$ 4 17
M Z $\hat{=}$ 12 25

C H $\hat{=}$ 2 7
G L $\hat{=}$ 6 11

$$\Rightarrow \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 17 \end{pmatrix} = \begin{pmatrix} 12 \\ 25 \end{pmatrix} \qquad \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 7 \end{pmatrix} = \begin{pmatrix} 6 \\ 11 \end{pmatrix}$$

$$\Rightarrow \quad 4a_{11} + 17a_{12} = 12 \quad \text{I} \qquad 2a_{11} + 7a_{12} = 6 \quad \text{III}$$

$$4a_{21} + 17a_{22} = 25 \quad \text{II} \qquad 2a_{21} + 7a_{22} = 11 \quad \text{IV}$$

Es entsteht also ein 4×4 - LGS, oder einfacher zwei 2×2 - LGS (I & III, II & IV), die nach den Komponenten des Schlüssels aufgelöst werden können.

Lösung: $a_{11} = 3$, $a_{12} = 0$, $a_{21} = 2$, $a_{22} = 1$

$$\Rightarrow \quad A = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}, \qquad \text{Schlüssel: } \underline{\text{D A C B}}$$

c) $\det(A) = 3$

$$A^{-1} = 9 \cdot \begin{pmatrix} 1 & 0 \\ -2 & 3 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 & 0 \\ -18 & 27 \end{pmatrix} \bmod 26 = \begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix}$$

D G Z L $\hat{=}$ 3 6 25 11

$$\begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 6 \end{pmatrix} \bmod 26 = \begin{pmatrix} 27 \\ 30 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \hat{=} \text{B E}$$

$$\begin{pmatrix} 9 & 0 \\ 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 25 \\ 1 \end{pmatrix} \bmod 26 = \begin{pmatrix} 225 \\ 201 \end{pmatrix} \bmod 26 = \begin{pmatrix} 17 \\ 19 \end{pmatrix} \hat{=} \text{R T}$$

BERT hat die Nachricht verschlüsselt!

e) Um einen Schlüssel der Länge 4 knacken zu können, muss man mind. 2 "Wörter" der Länge 2 chiffrieren können.
Allg.: Schlüssellänge $n \rightarrow \sqrt{n}$ Wörter der Länge $\sqrt{n}$. Dies wird sehr schnell unmöglich, wenn man nicht einen signifikanten Teil der Klartext-Nachricht bereits kennt.

Z1

S A | H A | R A

$\downarrow$ $\downarrow$ $\downarrow$

$\begin{pmatrix}18\\0\end{pmatrix}$ $\begin{pmatrix}7\\0\end{pmatrix}$ $\begin{pmatrix}17\\0\end{pmatrix}$

B U | N T

$\downarrow$

$A = \begin{pmatrix}1 & 20\\13 & 19\end{pmatrix}$

$$\begin{pmatrix}1 & 20\\13 & 19\end{pmatrix}\begin{pmatrix}18\\0\end{pmatrix} = \begin{pmatrix}18\\234\end{pmatrix} \bmod 26 = \begin{pmatrix}18\\0\end{pmatrix} \rightarrow \begin{matrix}S\\A\end{matrix}$$

$$\begin{pmatrix}1 & 20\\13 & 19\end{pmatrix}\begin{pmatrix}7\\0\end{pmatrix} = \begin{pmatrix}7\\91\end{pmatrix} \bmod 26 = \begin{pmatrix}7\\13\end{pmatrix} \rightarrow \begin{matrix}H\\N\end{matrix}$$

$$\begin{pmatrix}1 & 20\\13 & 19\end{pmatrix}\begin{pmatrix}17\\0\end{pmatrix} = \begin{pmatrix}17\\221\end{pmatrix} \bmod 26 = \begin{pmatrix}17\\13\end{pmatrix} \rightarrow \begin{matrix}R\\N\end{matrix}$$

Die Chiffre ist kritisch nahe am Klartext!

$$(\det A)^{-1} = \left((19 - 260) \bmod 26\right)^{-1} = \left((-241) \bmod 26\right)^{-1} = 19^{-1} = 11$$

$$A^{-1} = 11 \cdot \begin{pmatrix}19 & -20\\-13 & 1\end{pmatrix} \bmod 26 = \begin{pmatrix}1 & -220\\-143 & 11\end{pmatrix} \bmod 26 = \begin{pmatrix}1 & 14\\13 & 11\end{pmatrix}$$

$11 \cdot 19 \bmod 26 = 1$

$$\begin{pmatrix}1 & 14\\13 & 11\end{pmatrix}\begin{pmatrix}18\\0\end{pmatrix} = \begin{pmatrix}18\\234\end{pmatrix} \bmod 26 = \begin{pmatrix}18\\0\end{pmatrix} \rightarrow \begin{matrix}S\\A\end{matrix}$$ ✓

$$\begin{pmatrix}1 & 14\\13 & 11\end{pmatrix}\begin{pmatrix}7\\13\end{pmatrix} = \begin{pmatrix}189\\234\end{pmatrix} \bmod 26 = \begin{pmatrix}7\\0\end{pmatrix} \rightarrow \begin{matrix}H\\A\end{matrix}$$ ✓

$$\begin{pmatrix}1 & 14\\13 & 11\end{pmatrix}\begin{pmatrix}17\\13\end{pmatrix} = \begin{pmatrix}199\\364\end{pmatrix} \bmod 26 = \begin{pmatrix}17\\0\end{pmatrix} \rightarrow \begin{matrix}R\\A\end{matrix}$$ ✓

Z2

a) So, wie das Programm in A3a geschrieben ist, muss nur $n = 29$ gesetzt werden.
Alle Zahlen $\in \{1, \dots, 28\}$ haben nun eine modulare Inverse.

b) Die Chiffren können dann auch die Werte 26 bis 28 annehmen. Wie sollen sie in Text übersetzt werden?

c) Das Alphabet kann mit zusätzlichen Zeichen (z.B. Umlaute, Sonderzeichen) aufgefüllt werden.

Z3

individuelle Lösung. Hinweis: auf Z2 aufbauen!