Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 2

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 17. Oktober bis 25-27. Oktober
Verantwortlich: Roman Zorn

Aufgabe 1 : Knacken der affinen Chiffre

Gegeben ist folgender Ciphertext, der mit der affinen Chiffre und dem Schlüssel $(a, b) = (7, 13)$ verschlüsselt wurde:

`RDHQUXJQPI`

(a) ▶ Bestimmen Sie das inverse Element a^{-1} von a in $\mathbb{Z}_{26}^*$.

Lösungsvorschlag: ▶ Wir ermitteln a^{-1} wie in der Vorlesung mit dem erweiterten Euklidischen Algorithmus.

$n = 26$	$m = a = 7$	g	x	$y = a^{-1}$
26	7	1	3	-11
7	5	1	-2	3
5	2	1	1	-2
2	1	1	0	1
1	0	1	1	0

Es gilt also $a^{-1} = (-11) \equiv 15 \mod 26$, damit ist $a^{-1} = 15$ das gesuchte inverse Element.

(b) ▶ Entschlüsseln Sie den Ciphertext.

Lösungsvorschlag: ▶ Der Ciphertext ist (17 3 7 16 20 23 9 16 15 8). Für die Entschlüsselung berechnen wir für jedes Zeichen y im Ciphertext:

$$(a^{-1} \cdot (y - b)) \mod 26 \quad = \quad 15 \cdot (y - 13) \mod 26.$$

$$
\begin{aligned}
17: &\quad 15 \cdot (17 - 13) \mod 26 &&= 8 \\
3: &\quad 15 \cdot (3 - 13) \mod 26 &&= 6 \\
7: &\quad 15 \cdot (7 - 13) \mod 26 &&= 14 \\
16: &\quad 15 \cdot (16 - 13) \mod 26 &&= 19 \\
20: &\quad 15 \cdot (20 - 13) \mod 26 &&= 1 \\
23: &\quad 15 \cdot (23 - 13) \mod 26 &&= 20 \\
9: &\quad 15 \cdot (9 - 13) \mod 26 &&= 18 \\
16: &\quad 15 \cdot (16 - 13) \mod 26 &&= 19 \\
15: &\quad 15 \cdot (15 - 13) \mod 26 &&= 4 \\
8: &\quad 15 \cdot (8 - 13) \mod 26 &&= 3
\end{aligned}
$$

Der entschlüsselte Klartext ist also (8 6 14 19 1 20 18 19 4 3) bzw. `IGOTBUSTED`.

Aufgabe 2 : Affine Chiffre

Betrachten Sie die affine Chiffre aus der Vorlesung mit $M = C = \mathbb{Z}_{26}$.

(a) Begründen Sie für die folgenden Schlüssel, ob diese gültig sind.

(i) ▶ $(a_1, b_1) = (2, 10)$

(ii) ▶ $(a_2, b_2) = (7, 11)$

(iii) ▶ $(a_3, b_3) = (13, 14)$

Lösungsvorschlag: Für gültige Schlüssel $k = (a, b)$ muss $\text{ggT}(a, 26) = 1$ gelten. Demnach gilt:

- ▶ Schlüssel (i) ist ungültig, da $\text{ggT}(2, 26) = 2$,
- ▶ Schlüssel (ii) ist gültig, da $\text{ggT}(7, 26) = 1$, und
- ▶ Schlüssel (iii) ist ungültig, da $\text{ggT}(13, 26) = 13$.

(b) ▶ Verschlüsseln Sie den Klartext $m =$ `PINGUIN` mit dem Schlüssel $(a, b) = (9, 13)$.

Lösungsvorschlag: ▶ Wir berechnen für alle unterschiedlichen Zeichen

$$
\begin{aligned}
\texttt{P} \mathrel{\hat{=}} 15 \quad & E_{(9,13)}(15) = 9 \cdot 15 + 13 = 148 \equiv 18 \mod 26 && 18 \mathrel{\hat{=}} \texttt{S} \\
\texttt{I} \mathrel{\hat{=}} 8 \quad & E_{(9,13)}(6) = 9 \cdot 8 + 13 = 85 \equiv 7 \mod 26 && 7 \mathrel{\hat{=}} \texttt{H} \\
\texttt{N} \mathrel{\hat{=}} 13 \quad & E_{(9,13)}(13) = 9 \cdot 13 + 13 = 130 \equiv 0 \mod 26 && 0 \mathrel{\hat{=}} \texttt{A} \\
\texttt{G} \mathrel{\hat{=}} 6 \quad & E_{(9,13)}(6) = 9 \cdot 6 + 13 = 67 \equiv 15 \mod 26 && 15 \mathrel{\hat{=}} \texttt{P} \\
\texttt{U} \mathrel{\hat{=}} 20 \quad & E_{(9,13)}(20) = 9 \cdot 20 + 13 = 193 \equiv 11 \mod 26 && 11 \mathrel{\hat{=}} \texttt{L}
\end{aligned}
$$

Demnach lautet der Cipertext $c =$ `SHAPLHA`.

(c) Betrachten Sie den Klartext- und Ciphertextraum $\mathbb{Z}_{34}$.
► Geben Sie die Anzahl der gültigen Schlüssel $k = (a, b) \in \mathbb{Z}_{34} \times \mathbb{Z}_{34}$ an.

Lösungsvorschlag: ► Nach Vorlesung wissen wir, dass die Anzahl der gültigen Schlüssel $n \cdot \varphi(n)$ ist, wobei $\varphi(n)$ die Eulersche Phi-Funktion ist. Für $n = 34$ ergibt sich also

$$\begin{aligned} 34 \cdot \varphi(34) &= 34 \cdot (34 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{17})) \\ &= 34 \cdot 34 \cdot \frac{1}{2} \cdot \frac{16}{17} = 34 \cdot 16 \\ &= 544. \end{aligned}$$

Aufgabe 3 : Viginére-Chiffre

Betrachten Sie die Viginére-Chiffre aus der Vorlesung.

(a) ► Verschlüsseln Sie `SCHOKOLADENTORTE` mit dem Schlüssel `BALL`.

Lösungsvorschlag: ► Da der Schlüssel `BALL` 4 Zeichen lang ist, müssen wir den Klartext in Blöcke der Länge vier aufteilen:

`SCHO KOLA DENT ORTE` $\widehat{=}$ (18 2 7 14)(10 14 11 0)(3 4 13 19)(14 17 19 4)

Der Schlüssel `BALL` entspricht (1 0 11 11), aufaddiert (modulo 26) auf unseren Klartext ergibt das:

(19 2 18 25)(11 14 22 11)(4 4 24 4)(15 17 4 15) $\widehat{=}$ `TCSZ LOWL EEYE PREP`

Der Ciphertext lautet also $c =$ `TCSZLOWLEEYEPREP`.

(b) ► Wie sinnvoll ist der Schlüssel aus (a) gewählt? Begründen Sie Ihre Antwort.

Lösungsvorschlag: ► Die Probleme bei der Wahl des Schlüssels sind die gleichen wie die in der Vorlesung besprochenen Probleme (Schlüssel `ELLA`) zur Wahl des Schlüssels:

- Das `L` kommt doppelt vor, und
- das `A` lässt Buchstaben aus dem Klartext unverändert.

(c) Sie haben den Ciphertext `VQWWMFVIV` erhalten, für dessen Verschlüsselung der Schlüssel `EIS` verwendet wurde.
► Bestimmen Sie den Klartext.

Lösungsvorschlag: ► Das Entschlüsseln passiert analog zum Verschlüsseln, nur dass der Schlüssel hier abgezogen statt aufaddiert wird. Da der Schlüssel `EIS` 3 Zeichen lang ist, müssen wir den Ciphertext in Blöcke der Länge drei aufteilen:

$$\texttt{VQW WMF VIV} \;\widehat{=}\; (21\ 16\ 22)(22\ 12\ 5)(21\ 8\ 21)$$

Der Schlüssel `EIS` entspricht (4 8 18), subtrahiert (modulo 26) von unserem Ciphertext ergibt das:

$$(17\ 8\ 4)(18\ 4\ 13)(17\ 0\ 3) \;\widehat{=}\; \texttt{RIE SEN RAD}$$

Der Klartext lautet also $m = \texttt{RIESENRAD}$.

Aufgabe 4 : Matrizen

(a) ► Bilden Sie, wenn möglich, die multiplikative Inverse der Matrix

$$A_1 = \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix} \text{ in } \mathbb{Z}_5^{2\times 2}$$

Lösungsvorschlag: ► Es gilt:

$$\det \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix} = 3 \cdot 4 - 2 \cdot 2 = 12 - 4 = 8.$$

Da $\mathrm{ggT}\,(8, 5) = 1$ gilt, kann eine inverse Matrix berechnet werden. Es gilt

$$A_{adj} = \begin{pmatrix} 4 & -2 \\ -2 & 3 \end{pmatrix}$$

und $A^{-1} = (\det A)^{-1} A_{adj}$ mit $(\det A)^{-1} = 8^{-1} \equiv 3^{-1} \mod 5 \equiv 2 \mod 5$. Daher ist

$$A^{-1} = 2 \cdot \begin{pmatrix} 4 & -2 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \mod 5.$$

(b) ▶ Bilden Sie, wenn möglich, die multiplikative Inverse der Matrix

$$A_2 = \begin{pmatrix} 4 & 28 & 2 \\ 0 & 7 & 6 \\ 0 & 0 & 9 \end{pmatrix} \text{ in } \mathbb{Z}_{29}^{3\times 3}$$

Lösungsvorschlag: ▶ A_2 ist eine Dreiecksmatrix, damit ist ihre Determinante einfach das Produkt der Werte auf der Hauptdiagonalen: $\det(A_2) = 4 \cdot 7 \cdot 9 = 252 \equiv 20 \mod 29$. Mit $\text{ggT}(20, 29) = 1$ ist die Matrix invertierbar. Wir invertieren die Matrix nun mit dem aus "Lineare Algebra" bekannten Verfahren:

(I)	4	28	2	1	0	0	$\cdot 4^{-1} \equiv 22 \mod 29$
(II)	0	7	6	0	1	0	
(III)	0	0	9	0	0	1	
(I)	1	7	15	22	0	0	$-$(II)
(II)	0	7	6	0	1	0	
(III)	0	0	9	0	0	1	
(I)	1	0	9	22	28	0	$-$(III)
(II)	0	7	6	0	1	0	
(III)	0	0	9	0	0	1	
(I)	1	0	0	22	28	28	
(II)	0	7	6	0	1	0	$\cdot 7^{-1} \equiv 25 \mod 29$
(III)	0	0	9	0	0	1	
(I)	1	0	0	22	28	28	
(II)	0	1	5	0	25	0	
(III)	0	0	9	0	0	1	$\cdot 9^{-1} \equiv 13 \mod 29$
(I)	1	0	0	22	28	28	
(II)	0	1	5	0	25	0	$-(5 \cdot$ III$)$
(III)	0	0	1	0	0	13	
(I)	1	0	0	22	28	28	
(II)	0	1	0	0	25	22	
(III)	0	0	1	0	0	13	

$$\implies A^{-1} = \begin{pmatrix} 22 & 28 & 28 \\ 0 & 25 & 22 \\ 0 & 0 & 13 \end{pmatrix}$$

(c) ▶ (**Optional**) Wieviele unterschiedliche 2×2 Matrizen gibt es insgesamt, die in $\mathbb{Z}_3^{2\times 2}$ invertierbar sind?

Lösungsvorschlag: ▶ Invertierbar sind die Matrizen A mit $ggT\,(det(A), 3) = 1$, also jene mit $det(A) \in \{1, 2\} \pmod 3$. Insgesamt gibt es 48 Stück.

Wenn man nicht alle aufzählen will, konstruiert man die mit Determinante 0:

- Es gibt insgesamt $3^4 = 81$ Matrizen in $\mathbb{Z}_3^{2\times 2}$.
- Es gibt 3 Matrizen, bei denen alle Einträge gleich sind ($\Rightarrow$ Determinante 0), es bleiben also noch 78.
- Für $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ist die Determinante 0, wenn $a \cdot d \equiv b \cdot c \mod 3$
  - $\underline{a = 0}$: 2 Möglichkeiten für d, wenn $b = c = 0$ gilt oder je 3 Möglichkeiten für d, wenn entweder b oder c Null ist; insgesamt 14 Möglichkeiten
  - $\underline{d = 0}$: Analog: vertausche a und d: 14 Möglichkeiten - abzüglich 4, die schon im anderen Fall mit betrachtet wurden ($a = d = 0$).
  - $\underline{a = 1, d = 1}$: 1 Möglichkeit: $b = c = 2$
  - $\underline{a = 1, d = 2}$: 2 Möglichkeiten: $b = 1, c = 2$ oder $b = 2, c = 1$
  - $\underline{a = 2, d = 1}$: Analog: 2 Möglichkeiten
  - $\underline{a = 2, d = 2}$: 1 Möglichkeit: $b = c = 1$
- Insgesamt also $3+2\cdot 14-4+2\cdot 1+2\cdot 2 = 33$ unterschiedliche Möglichkeiten, die Determinante 0 zu erhalten.
- $\Longrightarrow$ $81 - 33 = 48$ Matrizen haben Determinante ungleich 0 und sind damit invertierbar.

Zur Veranschaulichung: alle 2×2 Matrizen in $\mathbb{Z}_3^{2\times 2}$:

$det(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}) = 0$
$det(\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 1 & 2 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix}) = 0$
$det(\begin{pmatrix} 0 & 0 \\ 2 & 2 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}) = 0$
$det(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}) = 1$
$det(\begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}) = 0$
$det(\begin{pmatrix} 0 & 2 \\ 0 & 2 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}) = 1$
$det(\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 0 & 2 \\ 2 & 2 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}) = 0$
$det(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}) = 1$
$det(\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}) = 2$
$det(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}) = 2$	$det(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}) = 2$
$det(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}) = 0$	$det(\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}) = 1$	$det(\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}) = 2$

$$det(\begin{pmatrix}1 & 1\\2 & 2\end{pmatrix}) = 0 \quad det(\begin{pmatrix}1 & 2\\0 & 0\end{pmatrix}) = 0 \quad det(\begin{pmatrix}1 & 2\\0 & 1\end{pmatrix}) = 1 \quad det(\begin{pmatrix}1 & 2\\0 & 2\end{pmatrix}) = 2$$
$$det(\begin{pmatrix}1 & 2\\1 & 0\end{pmatrix}) = 1 \quad det(\begin{pmatrix}1 & 2\\1 & 1\end{pmatrix}) = 2 \quad det(\begin{pmatrix}1 & 2\\1 & 2\end{pmatrix}) = 0 \quad det(\begin{pmatrix}1 & 2\\2 & 0\end{pmatrix}) = 2$$
$$det(\begin{pmatrix}1 & 2\\2 & 1\end{pmatrix}) = 0 \quad det(\begin{pmatrix}1 & 2\\2 & 2\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 0\\0 & 0\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 0\\0 & 1\end{pmatrix}) = 2$$
$$det(\begin{pmatrix}2 & 0\\0 & 2\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 0\\1 & 0\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 0\\1 & 1\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 0\\1 & 2\end{pmatrix}) = 1$$
$$det(\begin{pmatrix}2 & 0\\2 & 0\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 0\\2 & 1\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 0\\2 & 2\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 1\\0 & 0\end{pmatrix}) = 0$$
$$det(\begin{pmatrix}2 & 1\\0 & 1\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 1\\0 & 2\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 1\\1 & 0\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 1\\1 & 1\end{pmatrix}) = 1$$
$$det(\begin{pmatrix}2 & 1\\1 & 2\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 1\\2 & 0\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 1\\2 & 1\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 1\\2 & 2\end{pmatrix}) = 2$$
$$det(\begin{pmatrix}2 & 2\\0 & 0\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 2\\0 & 1\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 2\\0 & 2\end{pmatrix}) = 1 \quad det(\begin{pmatrix}2 & 2\\1 & 0\end{pmatrix}) = 1$$
$$det(\begin{pmatrix}2 & 2\\1 & 1\end{pmatrix}) = 0 \quad det(\begin{pmatrix}2 & 2\\1 & 2\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 2\\2 & 0\end{pmatrix}) = 2 \quad det(\begin{pmatrix}2 & 2\\2 & 1\end{pmatrix}) = 1$$
$$det(\begin{pmatrix}2 & 2\\2 & 2\end{pmatrix}) = 0$$