Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 2
26. Oktober 2018

Übungen zur Kryptographie
Lösung

Aufgabe 7

a) Die Komposition ist wohldefiniert auf $\mathrm{Aff}(2,\mathbb{Z}_{26})$, da für alle $\varphi,\psi \in \mathrm{Aff}(2,\mathbb{Z}_{26})$ gilt:

$$\begin{aligned}&\varphi(x) = Ax + t, \psi(x) = Bx + s \text{ für } A, B \in \mathrm{Gl}(2,\mathbb{Z}_{26}),\ s,t, \in \mathbb{Z}_{26}^2\\ &\Rightarrow \varphi(\psi(x)) = ABx + (As + t) \in \mathrm{Aff}(2,\mathbb{Z}_{26}).\end{aligned}$$

Das neutrale Element ist die Identität, das inverse Element zu φ ist $x \mapsto A^{-1}x - A^{-1}t$. Damit ist $\mathrm{Aff}(2,\mathbb{Z}_{26})$ eine Gruppe.

Mit dem chinesischen Restsatz wissen wir, dass $\mathbb{Z}_{26} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{13}$. Wir bestimmen die Anzahl der invertierbaren Elemente in $\mathrm{Gl}(k)$ für einen beliebigen endlichen Körper k mit p Elementen. Eine Matrix $A = (a_1, a_2) \in \mathrm{Gl}(k)$ ist genau dann invertierbar, wenn ihre Spalten a_1 und a_2 linear unabhängig sind. Für a_1 haben wir die Wahl $p^2 - 1$ (zwei Einträge ohne dem Nullvektor). Weiter soll gelten $a_2 \neq xa_1,\ x \in k$, also haben wir $p^2 - p$ Möglichkeiten. Insgesamt hat $\mathrm{Gl}(k)$ damit $(p^2-1)(p^2-p)$ Elemente. Ein Automorphimus von $\mathbb{Z}_2 \times \mathbb{Z}_{13}$ hat jetzt die Form

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$$

mit $\alpha \in \mathrm{End}(2,\mathbb{Z}_2),\ \delta \in \mathrm{End}(2,\mathbb{Z}_{13})$ und $\beta \in \mathrm{Hom}_2(\mathbb{Z}_{13},\mathbb{Z}_2), \gamma \in \mathrm{Hom}_2(\mathbb{Z}_2,\mathbb{Z}_{13})$. Aufgrund der verschiedenen Charakteristiken gilt $\beta,\gamma = 0$ also $\alpha \in \mathrm{Gl}(2,\mathbb{Z}_2),\ \delta \in \mathrm{Gl}(2,\mathbb{Z}_{13})$ und wir erhalten die Anzahl der Element von $\mathrm{Gl}(2,\mathbb{Z}_{26})$ zu

$$(2^2 - 1)(2^2 - 2)(13^2 - 1)(13^2 - 13) = 157248.$$

Die Gruppe $\mathrm{Aff}(2,\mathbb{Z}_{26})$ hat dann

$$26^2 \cdot 157248 = 106299648$$

Elemente. Hierbei haben wir verwendet, dass aus $Ax + t = Bx + s, \forall x \in \mathbb{Z}_{26}^2$ bereits für $x = 0 \Rightarrow s = t$ und somit $Ax = Bx, \forall x \in \mathbb{Z}_{26}^2$ folgt. Man kann die Anzahl der Elemente von $\mathrm{Gl}(2,\mathbb{Z}_{26})$ auch direkt bestimmen: Eine Matrix A ist genau dann invertierbar, wenn ihre Determinante invertierbar, d.h. eine Einheit, ist. $\mathbb{Z}_{26}$ besitzt die 12 Einheiten

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Sei $\det(A) = ad - bc$ die Determinante von $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. $\det(A) = u \in \mathbb{Z}_{26}^*$ kann nur gelten, wenn genau einer der Summanden ungerade ist. Wir bestimmen die Häufigkeiten mit der eine Zahl $m \in \mathbb{Z}_{26}$ als Produkt zweier Zahlen auftritt:

- 0 ergibt sich 75fach: $0 \cdot d$ für d beliebig, $a \cdot 0$ für $a \neq 0$ und $13 \cdot c$, $c \neq 0$ gerade, sowie $b \cdot 13$ mit $b \neq 0$ gerade.
- 13 erhält man auf 25 verschiedenen Weisen: $13 \cdot d$ für d ungerade und $a \cdot 13$ für $a \neq 13$ und ungerade.
- Jede gerade Zahlen ungleich 0 tritt 36fach auf, jede ungerade Zahl ungleich 13 genau 12fach.

Um den letzten Punkt zu verstehen beachte man, dass der Gruppenautomorphismus $\mathbb{Z}_{26} \to \mathbb{Z}_{26}, x \mapsto 7 \cdot x$ genau die Mengen $\mathbb{Z}_{26}^*, (2) \setminus \{0\}, \{0\}, \{13\}$ erhält. Somit gilt $(7^k a, d) = (7^k a', d')$ für zwei Lösung von $7^k ad = 7^k m = 7^k a' d'$ genau dann wenn $d = d', 7^k a = 7^k a' \Leftrightarrow a = a', d = d'$. Es folgt

$$\frac{13 \cdot 39 - 75}{12} = 36, \quad \frac{13 \cdot 13 - 25}{12} = 12.$$

wobei wir die Anzahl der Lösungen (a, d) von $a \cdot d = m$ gerade und ungleich 0 durch die Anzahl der Elemente von $(2) \setminus \{0\}$ geteilt haben. Dies ist möglich da wir wissen, dass es für jedes $m \in (2) \setminus \{0\}$ gleich viele Lösungen von $a \cdot d = m$ gibt. Analog verfahren wir mit $m \in \mathbb{Z}_{26}^*$.
Wir bekommen einen Faktor 2 für die Wahl zwischen ad oder bc ungerade. Es gibt 12^2 Paare ungerader Zahlen. Jedoch sind nur $11 \cdot 36 + 75$ der Summen $\neq 13$. Also haben wir bereits

$$2 \cdot 12^2 \cdot (11 \cdot 36 + 75)$$

Lösungen gefunden. Wie wir gesehen haben gibt es weitere 25 Möglichkeiten eine ungerade Zahl mit Teiler 13 zu kombinieren. Der zugehörige gerade Summand darf nicht 0 werden, also weitere $12 \cdot 36$ Möglichkeiten. Insgesamt also wie erwartet

$$2 \cdot 12^2 \cdot (11 \cdot 36 + 75) + 2 \cdot 25 \cdot 12 \cdot 36 = 157248.$$

b) Man identifiziere

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
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

Damit müssen wir A, t wie zuvor finden mit

$$A \cdot \begin{pmatrix} 0 & 1 & 17 \\ 11 & 4 & 19 \end{pmatrix} + (t, t, t) = \begin{pmatrix} 9 & 18 & 15 \\ 14 & 4 & 7 \end{pmatrix}$$

Subtrahiert man die zweite resp. dritte Spalte von der ersten so erhält man

$$A \cdot \begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix} = \begin{pmatrix} -9 & -6 \\ 10 & 7 \end{pmatrix}$$

Wir erkennen $\det \begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix} = -3 \in \mathbb{Z}_{26}^*$ und

$$\begin{pmatrix} -1 & 9 \\ 7 & -8 \end{pmatrix}^{-1} = 17 \cdot \begin{pmatrix} -8 & -9 \\ -7 & -1 \end{pmatrix} = \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix}.$$

Schließlich ist

$$A = \begin{pmatrix} -9 & -6 \\ 10 & 7 \end{pmatrix} \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix} = \begin{pmatrix} 14 & -3 \\ 17 & 15 \end{pmatrix}.$$

Es folgt

$$A \begin{pmatrix} 0 & 1 & 17 \\ 11 & 4 & 19 \end{pmatrix} - \begin{pmatrix} 9 & 10 & 15 \\ 14 & 4 & 7 \end{pmatrix} = \begin{pmatrix} -7 & 2 & -1 \\ 9 & -1 & 2 \end{pmatrix} - \begin{pmatrix} 9 & 18 & 15 \\ 14 & 4 & 7 \end{pmatrix} = \begin{pmatrix} -16 & -16 & -16 \\ -5 & -5 & -5 \end{pmatrix}.$$

Damit haben wir eine eindeutige affine Abbildung gefunden, die `ALBERT` in `JOSEPH` überführt.
Für den Code `JOHANN` verfahren wir analog:

$$A \cdot \begin{pmatrix} 0 & 1 & 17 \\ 11 & 4 & 19 \end{pmatrix} + (t, t, t) = \begin{pmatrix} 9 & 7 & 13 \\ 14 & 0 & 13 \end{pmatrix}$$

und

$$A = \begin{pmatrix} 2 & -4 \\ 14 & 1 \end{pmatrix} \begin{pmatrix} -6 & 3 \\ 11 & 9 \end{pmatrix} = \begin{pmatrix} -4 & -4 \\ 5 & -1 \end{pmatrix}$$

Es folgt

$$A \begin{pmatrix} 0 & 1 & 17 \\ 11 & 4 & 19 \end{pmatrix} - \begin{pmatrix} 9 & 7 & 13 \\ 14 & 0 & 13 \end{pmatrix} = \begin{pmatrix} 8 & 6 & 12 \\ -11 & 1 & 14 \end{pmatrix} - \begin{pmatrix} 9 & 7 & 13 \\ 14 & 0 & 13 \end{pmatrix} = \begin{pmatrix} -1 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Damit haben wir eine passende Abbildung gefunden allerdings ist A hier nicht invertierbar- $\det(A) = 24 \notin \mathbb{Z}_{26}^{\times}$.

Aufgabe 8

a) Wir betrachten die Menge der Paare $\Omega' = \{(X, Y) \in \mathfrak{A} \times \in \mathfrak{A}\}$. Die Wahrscheinlichkeit ein Diagonalelement zu ziehen beträgt gerade $\sum_{i=1}^{m} p_i^2$. Wir erhalten ein Bernoulliexperiment mit $P = \sum_{i=1}^{m} p_i^2$ für „ein Paar wird gezogen“. Es gilt

$$\begin{aligned} \mathbb{E}(\kappa(X, Y)) &= \sum_{k=1}^{N} \frac{k}{N} P(k \text{ Paare}) = \sum_{k=1}^{N} \frac{k}{N} \binom{N}{k} P^k (1-P)^{N-k} \\ &= P \sum_{k=0}^{N-1} \binom{N}{k} P^k (1-P)^{N-1-k} = P(P + 1 - P)^{N-1} = P. \end{aligned}$$

b) Wir setzen ein

$$\begin{aligned} \Phi(X) &= \frac{1}{N-1} \sum_{k=1}^{N} \kappa(X, \varrho^k(X)) = \frac{1}{N(N-1)} \sum_{j=1}^{m} \sum_{k=1}^{N} \delta(x_j, x_{j+k}) \\ &= \frac{1}{N(N-1)} \sum_{j=1}^{m} f_j(f_j - 1) \end{aligned}$$

wobei $f_j - 1$ gerade die Kopien von x_j sind und diese werden für jedes der f_j x_j durchlaufen.

c) Folgt trivial aus b), da sich nur die Summationsreihenfolge ändert:

$$\Phi(\sigma(X)) = \frac{1}{N(N-1)} \sum_{j=1}^{m} f_{\sigma^{-1}(j)}(f_{\sigma^{-1}(j)} - 1) = \frac{1}{N(N-1)} \sum_{j=1}^{m} f_j(f_j - 1) = \Phi(X).$$