Kap. II: Monoalphabetische Verschlüsselungen

§ 4. Affine Chiffre

A) Additive Chiffre (Verschiebe–Chiffre)

Wir wollen jetzt die schon mehrfach behandelte Verschiebe–Chiffre formelmäßig in den Griff bekommen. Zu diesem Zweck nummerieren wir die Buchstaben–Alphabete.

(4.1) DEF: a) Die Nummerierung der Buchstaben des Klartextalphabets $\mathfrak{a} = \{a, b, c, \ldots, z\}$ mit den Zahlen von 0 bis 25 liefert die bijektive Abbildung

$$\omega : \mathfrak{a} \longrightarrow \mathcal{R}_{26} ,$$

wobei $\mathcal{R}_{26}$ die Menge der natürlichen Zahlen von 0 bis 25 ist.

b) Die Nummerierung der Buchstaben des Geheimtextalphabets $\mathfrak{A} = \{A, B, C, \ldots, Z\}$ mit den Zahlen von 0 bis 25 liefert die bijektive Abbildung

$$\Omega : \mathfrak{A} \longrightarrow \mathcal{R}_{26} .$$

(4.2) SATZ: Sei $\mathcal{R}_{26} = \{0, 1, 2, 3, \ldots, 25\}$. Für $k \in \mathbb{Z}$ sei die Abbildung

$$\varepsilon_k : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$$

definiert durch

$$\varepsilon_k(r) := (r + k) \bmod 26 \quad (r \in \mathcal{R}_{26}) .$$

Dann gilt:

a) ε_k ist bijektiv mit der Umkehrabbildung $\varepsilon_{-k} : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$, d.h.

$$(\varepsilon_k)^{-1} = \varepsilon_{-k} .$$

b) $\varepsilon_0 = \mathrm{id}_{\mathcal{R}_{26}}$

c) $k, l \in \mathbb{Z}$: $\varepsilon_k = \varepsilon_l \iff k \bmod 26 = l \bmod 26$.

(4.3) FOLGERUNG: Für jedes $k \in \mathbb{Z}$ ist

$$V_k := \Omega^{-1} \circ \varepsilon_k \circ \omega : \mathfrak{a} \longrightarrow \mathfrak{A}$$

eine bijektive Abbildung mit der Umkehrabbildung

$$(V_k)^{-1} := \omega^{-1} \circ \varepsilon_{-k} \circ \Omega : \mathfrak{A} \longrightarrow \mathfrak{a} .$$

(4.4) BEM: **a)** Jede der bijektiven Abbildungen $V_k : \mathfrak{a} \longrightarrow \mathfrak{A}$ läßt sich zum Verschlüsseln benutzen. Man nennt V_k eine **additive Chiffre** oder eine **Verschiebe–Chiffre**. Mit der Umkehrabbildung $(V_k)^{-1} : \mathfrak{A} \longrightarrow \mathfrak{a}$ wird die Entschlüsselung vorgenommen.

b) $k = 3$ liefert die ursprüngliche **Caesar–Verschlüsselung** V_3.

c) Wegen(4.2c) gibt es genau 26 additive Chiffre V_k $(k \in \mathcal{R}_{26})$, von denen V_0 uninteressant ist.

B) Multiplikative Chiffre

Wir betrachten jetzt für $k \in \mathbb{Z}$ die Abbildung

$$\mu_k : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}\ ,\ \mu_k(r) := (r \cdot k) \bmod 26 \quad (r \in \mathcal{R}_{26})\,.$$

Als erstes untersuchen wir, ob μ_k immer eine bijektive Abbildung ist.

(4.5) BEISPIELE: **a)** $\mu_1 = \mathrm{id}_{\mathcal{R}_{26}}$ ist bijektiv.

b) μ_2 ist nicht injektiv und damit auch nicht bijektv.

Es ist $\mu_2(0) = 0 = \mu_2(13)$ mit $0 \neq 13$.

c) μ_3 ist bijektiv (s. Aufg. 12a).

(4.6) SATZ: **a)** Sei $k \in \mathbb{Z}$. Die Abbildung $\mu_k : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$ ist genau dann bijektiv, wenn k und 26 teilerfremd sind, d.h. wenn $\mathrm{ggT}(k, 26) = 1$ gilt.

b) Im Falle $\mathrm{ggT}(k, 26) = 1$ gibt es ein $m \in \mathbb{Z}$ mit der Eigenschaft $(k \cdot m) \bmod 26 = 1$, und μ_m ist die Umkehrabbildung von μ_k.

$$(\mu_k)^{-1} \ = \ \mu_m\,.$$

Eine ganze Zahl m mit $(k \cdot m) \bmod 26$ heißt ein **Inverses von k modulo 26**.

c) Für $k, l \in \mathbb{Z}$ gilt: $\mu_k = \mu_l \iff k \bmod 26 = l \bmod 26$.

(4.7) FOLGERUNG: Für jedes $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k, 26) = 1$ ist die Abbildung

$$M_k := \Omega^{-1} \circ \mu_k \circ \omega : \mathfrak{a} \longrightarrow \mathfrak{A}$$

bijektiv mit der Umkehrabbildung

$$(M_k)^{-1} := \omega^{-1} \circ \mu_m \circ \Omega : \mathfrak{A} \longrightarrow \mathfrak{a}\,,$$

wobei m ein Inverses von k modulo 26 ist.

Die mit M_k vorgenommene Verschlüsselung heißt **multiplikative Chiffre**.

Es gibt genau 12 multiplikative Chiffre, von denen M_1 uninteressant ist.

C) Affine Chiffre

Eine affine Chiffre ist eine Hintereinanderausführung einer additiven und einer multiplikativen Chiffre.

Für $k, l \in \mathbb{Z}$ sei die Abbildung $\eta_{k,l} : \mathcal{R}_{26} \longrightarrow \mathcal{R}_{26}$ definiert durch

$$\eta_{k,l} := \varepsilon_k \circ \mu_l \,.$$

Beispiele: $\eta_{3,5}$ und $\eta_{4,6}$ haben die folgenden Wertetabellen:

r	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
$\eta_{3,5}(r)$	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0	5	10	15	20	25	4	9	14	19	24
$\eta_{4,6}(r)$	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24

Aus der Wertetabelle geht unmittelbar hervor, dass $\eta_{3,5}$ bijektiv ist, wohingegen $\eta_{4,6}$ nicht bijektiv ist.

(4.8) SATZ: Seien $k, l, m, n \in \mathbb{Z}$. Dann gilt:

a) $\eta_{k,l}(r) \;=\; (k + l \cdot r) \bmod 26$ für alle $r \in \mathcal{R}_{26}$

b) $\eta_{k,l}$ ist genau dann bijektiv, wenn $\mathrm{ggT}(l, 26) = 1$ gilt.

c) Im Falle $\mathrm{ggT}(l, 26) = 1$ ist

$$(\eta_{k,l})^{-1} \;=\; \mu_m \circ \varepsilon_n \,,$$

wobei m ein Inverses von l modulo 26 und $n := (-k) \bmod 26$ ist.

d) $\eta_{k,l} = \eta_{m,n} \iff (k \bmod 26 = m \bmod 26$ und $l \bmod 26 = n \bmod 26) \,.$

(4.9) FOLGERUNG: Seien $k, l \in \mathbb{Z}$. Im Falle $\mathrm{ggT}(l, 26) = 1$ ist die Abbildung

$$A_{k,l} := \Omega^{-1} \circ \eta_{k,l} \circ \omega : \mathfrak{a} \longrightarrow \mathfrak{A}$$

bijektiv mit der Umkehrabbildung

$$(A_{k,l})^{-1} := \omega^{-1} \circ (\mu_m \circ \varepsilon_n) \circ \Omega : \mathfrak{A} \longrightarrow \mathfrak{a} \,,$$

wobei m ein Inverses von l modulo 26 und $n := (-k) \bmod 26$ ist.

Die mit $A_{k,l}$ vorgenommene Verschlüsselung heißt **affine Chiffre**.

(4.10) BEM: **a)** Es gibt genau $\mathbf{26 \cdot 12 = 312}$ affine Chiffre, von denen $\boldsymbol{A_{0,1}}$ uninteressant ist.

b) Im allgemeinen gilt $\varepsilon_k \circ \mu_l \neq \mu_l \circ \varepsilon_k$.

c) $\{ \varepsilon_k \circ \mu_l \mid k, l \in \mathbb{Z} \} = \{ \mu_n \circ \varepsilon_m \mid m, n \in \mathbb{Z} \}$.

d) Die beiden Abbildungen $\Omega \circ M_l : \mathfrak{a} \longrightarrow \mathcal{R}_{26}$ und $V_k \circ \omega^{-1} : \mathcal{R}_{26} \longrightarrow \mathfrak{A}$ lassen sich hintereinanderausführen. Es ist

$$(V_k \circ \omega^{-1}) \circ (\Omega \circ M_l) : \mathfrak{a} \longrightarrow \mathfrak{A}$$

eine Abbildung von $\mathfrak{a}$ nach $\mathfrak{A}$, für die gilt:

$$(V_k \circ \omega^{-1}) \circ (\Omega \circ M_l) = (\Omega^{-1} \circ \varepsilon_k \circ \omega \circ \omega^{-1}) \circ (\Omega \circ \Omega^{-1} \circ \mu_k \circ \omega) = \Omega^{-1} \circ \varepsilon_k \circ \mu_k \circ \omega = A_{k,l}\,.$$

In diesem Sinne kann man $A_{k,l}$ als "Hintereinanderausführung" von V_k und M_l auffassen.