Kap. III: Polyalphabetische Verschlüsselungsverfahren

§ 6. Die homophone Chiffre

(6.1) DEF: Ein Verschlüsselungsverfahren heißt **polyalphabetisch**, wenn ein Buchstabe aus dem Klartextalphabet auch durch mehrere Buchstaben aus dem Geheimtextalphabet verschlüsselt werden kann.

Bei einer **homophonen Verschlüsselung** (homophon bedeutet gleichlautend) eines Klartextes treten die Geheimtextbuchstaben alle mit ungefähr dergleichen Häufigkeit auf, so dass eine Häufigkeitsanalyse nur mit einem sehr viel größeren Aufwand durchgeführt werden kann, wenn sie überhaupt zum Ziele führt.

Dies kann man dadurch erreichen, dass man einen Klartextbuchstaben durch ungefähr so viele Buchstaben des Geheimtextalphabetes ersetzt, wie es der Häufigkeit dieses Buchstaben entspricht. Dabei muss man darauf achten, dass zwei verschiedene Klartextbuchstaben nicht durch denselben Buchstaben verschlüsselt werden, damit eine eindeutige Entschlüsselung möglich ist.

Die homophone Chiffre ist eine polyalphabetische Verschlüsselung.

(6.2) Beispiel für eine homophone Chiffre (aus Beutelspacher: Kryptologie)

Als Klartextalphabet wählen wir $\mathfrak{a} = \{a, b, c, \ldots, x, y, z\}$ und als Geheimtextalphabet

$$\mathcal{G} := \{00, 01, 02, \ldots, 09, 10, 11, 12, \ldots, 97, 98, 99\}\,.$$

Es ist $|\mathcal{G}| = 100$. Wir orden jedem Buchstaben aus $\mathfrak{a}$ soviele Buchstaben aus $\mathcal{G}$ zu, wie es ungefähr der Häufigkeit dieses Buchstabens nach der Tabelle (5.10) entspricht, d.h. wir bilden für jeden Buchstaben $\gamma \in \mathfrak{a}$ eine nichtleere Teilmenge $\mathcal{G}_\gamma \subseteq \mathcal{G}$ von möglichen Verschlüsselungsbuchstaben für γ. So ist z.B. (s. Tabelle auf der näechsten Seite)

$$\mathcal{G}_a = \{10, 21, 52, 59, 71\}$$
$$\mathcal{G}_g = \{08, 12, 97\}$$
$$\mathcal{G}_q = \{25\}\,.$$

Diese Teilmengen sind nichtleer, paarweise disjunkt und ihre Vereinigung ist ganz $\mathcal{G}$.

Buchstabe	**mögliche Geheimtextzeichen**
a	10 21 52 59 71
b	20 34
c	28 06 80
d	04 19 70 81 87
e	09 18 33 38 40 42 53 54 55 60 66 75 85 86 92 93 99
f	00 41
g	08 12 97
h	07 24 47 89
i	14 39 46 50 65 76 88 94
j	57
k	23
l	16 03 84
m	27 11 49
n	30 35 43 62 63 67 68 72 77 79
o	02 05 82
p	31
q	25
r	17 36 51 69 74 78 83
s	15 26 45 56 61 73 96
t	13 32 90 91 95 98
u	29 01 58
v	37
w	22
x	44
y	48
z	64

Beispiel für eine Verschlüsselung: Klartext: universitaet paderborn

Bei der Verschlüsselung wählen wir für jeden Klartextbuchstaben γ einen Buchstaben aus $\mathcal{G}_\gamma$, wobei wir darauf achten, dass γ ggfs. durch unterschiedliche Buchstaben aus $\mathcal{G}_\gamma$ verschlüsselt wird. Wir können entweder einen Buchstaben aus $\mathcal{G}_\gamma$ **zufällig** auswählen oder wir gehen in einer bestimmten, sich wiederholenden Reihenfolge vor.

Verschlüsselung: 01624693745688325933913171709917340551 68

Es gibt noch viele weitere Möglichkeiten, den Klartext zu verschlüsseln, da etwa der Buchstabe a zu einem der 5 angegebenen Geheimtextzeichen verschlüsselt werden kann. Die Entschlüsselung ist aber eindeutig, da die Mengen der Geheimtextzeichen für verschiedene Buchstaben disjunkt sind (d.h. leeren Durchschnitt haben) .

(6.3) BEM: Bei einer **homophonen Verschlüsselung** des Klartextalphabets

$$\mathfrak{a} = \{a, b, c, \ldots, x, y, z\}$$

durch ein Geheimtextalphabet $\mathcal{G}$ ist für jeden Buchstaben $\gamma \in \mathfrak{a}$ eine Teilmenge

$$\mathcal{G}_\gamma \subseteq \mathcal{G}$$

gegeben mit folgenden Eigenschaften:

1) Für alle $\gamma \in \mathfrak{a}$ gilt $\mathcal{G}_\gamma \neq \emptyset$

2) Für alle $\gamma, \delta \in \mathfrak{a}$ mit $\gamma \neq \delta$ gilt $\mathcal{G}_\gamma \cap \mathcal{G}_\delta = \emptyset$

3) $\bigcup\limits_{\gamma \in \mathfrak{a}} \mathcal{G}_\gamma = \mathcal{G}$

4) $|\mathcal{G}_\gamma| \approx \dfrac{x}{100} \cdot |\mathcal{G}|$, wobei die x die Häufigkeit von γ aus der Tabelle (5.10) ist.

Verschlüsselt wird ein Buchstabe $\gamma \in \mathfrak{a}$ dadurch, dass man (zufällig) einen Buchstaben aus $\mathcal{G}_\gamma$ auswählt, was wegen 1) immer möglich ist. Zu einem Geheimtextbuchstaben $\Gamma \in \mathcal{G}$ findet man wegen 3) und 2) einen eindeutig bestimmten Buchstaben $\gamma \in \mathfrak{a}$ mit $\Gamma \in \mathcal{G}_\gamma$ und dieser Buchstabe γ ist dann die Entschlüsselung von Γ . 4) garantiert, dass alle Buchstaben im Geheimtext ungefähr gleich häufig vorkommen.

Eine Entschlüsselung einer homophonen Chiffre ohne Kenntnis des Schlüssels kann man mit verfeinerten Methoden einer Häufigkeitsanalyse versuchen.