

## 1.2 Beispiele für Mehrfach-Chiffren

### Beispiele für Gruppen

Jeweils eine Gruppe bilden die folgenden längentreuen Blockchiffren:

- die Verschiebechiffren über  $\Sigma$  bezüglich einer Gruppenstruktur auf  $\Sigma$ ,
- die monoalphabetischen Substitutionen über  $\Sigma$ ,
- die BELASO-Chiffren fester Periode,
- die Block-Transpositionen fester Länge.

### DES

DES ist eine Blockchiffre auf  $\mathbb{F}_2^{64}$  mit Schlüsselraum  $\mathbb{F}_2^{56}$ . CAMPBELL und WIENER haben gezeigt (CRYPTO 92), dass DES die alternierende Gruppe der Ordnung  $2^{64}$  erzeugt.

### Historische Beispiele

Die Komposition einer polyalphabetischen Chiffre der Periode  $l$  mit einer der Periode  $q$  hat die Periode  $\text{kgV}(l, q)$ . **Anwendung:** Schlüsselerzeugermaschinen, wie sie in Kapitel I am Ende des Abschnitts über Chiffrierzylinder (I.4.8) kurz erwähnt wurden.

Weiteres historisches Beispiel: Die doppelte Spaltentransposition, die wesentlich schwerer zu brechen ist, als die einfache.

### Komposition von BELASO-Chiffren

Die Komposition zweier BELASO-Chiffren der Perioden  $l$  und  $q$  hat zwar die Periode  $\text{kgV}(l, q)$ , also im wesentlichen das Produkt  $lq$ , die Sicherheit entspricht aber höchstens der Summe  $l + q$ , wenn man einen Angriff mit bekanntem Klartext berücksichtigt:

Aus einem bekannten Klartext der Länge  $l + q$  gewinnt man  $l + q$  lineare Gleichungen für die ebensovielen Unbekannten, aus denen die beiden Schlüssel insgesamt bestehen. Sei dazu o. B. d. A.  $l < q$ . Dann haben wir die Situation

Klartext	$a_0$	$a_1$	...	$a_{l-1}$	$a_l$	...	$a_{q-1}$	...
Schlüssel 1	$h_0$	$h_1$	...	$h_{l-1}$	$h_0$	...	...	...
Schlüssel 2	$k_0$	$k_1$	...	$k_{l-1}$	$k_l$	...	$k_{q-1}$	...
Geheimtext	$c_0$	$c_1$	...	$c_{l-1}$	$c_l$	...	$c_{q-1}$	...

Wir haben also eine BELASO-Chiffre mit dem Gesamtschlüssel

$$(h_0 + k_0, h_1 + k_1, \dots)$$

und der Periode  $\text{kgV}(l, q)$ .

Nehmen wir nun bekannten Klartext der Länge  $l + q$  an, etwa o. B. d. A.  $(a_0, \dots, a_{l+q-1})$ . Dann haben wir das folgende lineare Gleichungssystem für die  $l + q$  Unbekannten  $h_0, \dots, h_{l-1}, k_0, \dots, k_{q-1} \in \mathbb{Z}/n\mathbb{Z}$ :

$$\begin{aligned} h_0 + k_0 &= c_0 - a_0, \\ h_1 + k_1 &= c_1 - a_1, \\ &\vdots \\ h_{l-1} + k_{l-1} &= c_{l-1} - a_{l-1}, \\ h_0 + k_l &= c_l - a_l, \\ &\vdots \\ h_{l+q-1 \bmod l} + k_{l+q-1 \bmod q} &= c_{l+q-1} - a_{l+q-1}. \end{aligned}$$

Dieses ist mit Sicherheit nicht eindeutig lösbar: Addiert man einen festen Wert  $x$  zu allen  $h_i$  und subtrahiert  $x$  von allen  $k_j$ , so hat man ebenfalls eine Lösung. Daher kann man zunächst der Einfachheit halber  $h_0 = 0$  annehmen; sollten die Schlüssel nicht zufällig gewählt, sondern aus Schlüsselwörtern gebildet sein, kann man am Ende mit einer einfachen „CAESAR-Exhaustion“ wie ganz am Anfang von Kapitel I die „wahren“ Schlüssel ermitteln. Für die Dechiffrierung tun es auch die verschobenen Schlüssel. Und da wir eine Unbekannte weniger haben, reichen im allgemeinen sogar  $l + q - 1$  bekannte Klartext-Zeichen, um die übrigen  $l + q - 1$  Gleichungen eindeutig aufzulösen. Dies soll hier nicht weiter ausgeführt werden; der Interessierte möge die folgende Aufgabe lösen.

### Übungsaufgabe

Gegeben sei der Geheimtext.

CIFRX KSYCI IDJZP TINUV GGKBD CWBFB CGWBC UXSJN LJFMC  
LQAZV TRLFV CPGYK MRUHO UZCIV NEOPP LK

Für einen Angriff mit bekanntem Klartext

- bestehe die berechtigte Vermutung, dass der Klartext mit „Sehr geehrter ...“ beginnt,
- seien mit Trial & Error plausible Schlüssellängen ausprobiert; es sei  $42 = 6 \times 7$  an der Reihe, um zu testen, ob eine doppelte BELASO-Verschlüsselung mit den Schlüssellängen 6 und 7 vorliegt.

(Hierzu braucht man nicht alle Schlüssellängen und Kombinationen durchzuprobieren; die Koinzidenzanalyse ist wegen der Kürze des Textes nicht allzu spezifisch, reicht aber, um alle bis auf wenige plausible Schlüssellängen auszuschließen.)