Ähnlichkeit von Chiffren[1]

Sei Σ ein Alphabet, $M \subseteq \Sigma^*$ eine Sprache und K eine endliche Menge (die als Schlüsselraum verwendet wird).

Definition [Shannon 1949]. Seien $F = (f_k)_{k\in K}$ und $\tilde{F} = (\tilde{f}_k)_{k\in K}$ Chiffren auf M, also

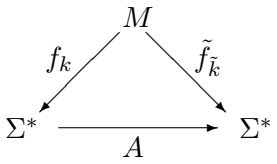
$$f_k, \tilde{f}_k \colon M \longrightarrow \Sigma^* \quad \text{für alle } k \in K.$$

Dann heißt F auf $\tilde{F}$ reduzierbar, wenn es eine Bijektion $A \colon \Sigma^* \longrightarrow \Sigma^*$ gibt mit

$$A \circ f \in \tilde{F} \quad \text{für alle } f \in F.$$

Das heißt, zu jedem $k \in K$ gibt es ein $\tilde{k} \in K$ mit $A \circ f_k = \tilde{f}_{\tilde{k}}$.

Ferner heißen F und $\tilde{F}$ ähnlich, wenn F auf $\tilde{F}$ und $\tilde{F}$ auf F reduzierbar ist.



Anwendung. Die Chiffren F und $\tilde{F}$ sind dann kryptoanalytisch äquivalent – vorausgesetzt natürlich, dass die Umrechnung $f \mapsto \tilde{f}$ effizient durchführbar ist.

Beispiele

1. **Reverser** Caesar**.** Dies ist eine monoalphabetische Substitution mit einem zyklisch verschobenen Exemplar des reversen Alphabets `ZY...BA`, z. B.

   ```
   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
   W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
   ```

   Es ist $K = \Sigma = \mathbb{Z}/n\mathbb{Z}$; sei $\rho(s) := n - s$ die Umkehrung des Alphabets (Reversion). Dann ist die Chiffre definiert durch

   $$f_k(s) := k - s \quad \text{für alle } k \in K.$$

   Diese Chiffre ist übrigens involutorisch: $f_k \circ f_k(s) = k - (k - s) = s$. Die gewöhnliche Caesar-Chiffre ist

   $$\tilde{f}_k(s) := k + s \quad \text{für alle } k \in K.$$

[1] Klaus Pommerening, Kryptologie; 20. Juni 2002, letzte Änderung: 16. Januar 2005

Dann ist

$$\rho \circ f_k(s) = \rho(k-s) = n+s-k = (n-k)+s = \tilde{f}_{n-k}(s),$$

also $\rho \circ f_k = \tilde{f}_{\rho(k)}$; da es auch eine entsprechende umgekehrte Gleichung gibt, *sind* CAESAR *und reverser* CAESAR *ähnlich.*

2. **Die** BEAUFORT**-Chiffre** [SESTRI 1710]. Dies ist eine periodische polyalphabetische Substitution mit einem Schlüssel $k = (k_0, \ldots, k_{l-1}) \in \Sigma^l$ (periodisch fortgesetzt):

$$f_k(a_0, \ldots, a_{r-1}) := (k_0 - a_0, k_1 - a_1, \ldots, k_{r-1} - a_{r-1}).$$

Sie ist, wie der reverse CAESAR, involutorisch. Die Alphabet-Tafel über dem Alphabet $\Sigma = \{\texttt{A}, \ldots, \texttt{Z}\}$ ist

```
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
-------------------------------------------------
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A
Y X W V U T S R Q P O N M L K J I H G F E D C B A Z
X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
H G F E D C B A Z Y X W V U T S R Q P O N M L K J I
G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
D C B A Z Y X W V U T S R Q P O N M L K J I H G F E
C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
B A Z Y X W V U T S R Q P O N M L K J I H G F E D C
A Z Y X W V U T S R Q P O N M L K J I H G F E D C B
```

Zum Vergleich die Trithemius-Belaso-Chiffre:

$$\tilde{f}_k(a_0, \ldots, a_{r-1}) := (k_0 + a_0, k_1 + a_1, \ldots, k_{r-1} + a_{r-1}).$$

Dann gilt wie beim reversen Caesar $\rho \circ f_k = \tilde{f}_{\rho(k)}$, und ebenso folgt: *Die* Beaufort-*Chiffre ist zur* Trithemius-Belaso-*Chiffre ähnlich.*

3. **Die Autokey-Chiffre.** Als Alphabet wird $\Sigma = \mathbb{Z}/n\mathbb{Z}$ genommen. Das Verschlüsselungsschema wird so aufgeschrieben:

$$\begin{array}{rcl|rcl|rcl}
c_0 & = & a_0 + k_0 & & & & & & \\
c_1 & = & a_1 + k_1 & & & & & & \\
\vdots & & & & & & & & \\
c_l & = & a_l + a_0 & c_l - c_0 & = & a_l - k_0 & & & \\
\vdots & & & & & & & & \\
c_{2l} & = & a_{2l} + a_l & c_{2l} - c_l & = & a_{2l} - a_0 & c_{2l} - c_l + c_0 & = & a_{2l} + k_0 \\
\vdots & & & & & & & &
\end{array}$$

Sei also

$$A(c_0, \ldots, c_i, \ldots, c_{r-1}) = (\ldots, c_i + c_{i-l} + c_{i-2l} - \ldots, \ldots);$$

exakt geschrieben sieht die i-te Komponente des Bildvektors so aus:

$$\sum_{j=0}^{\lfloor i \rfloor} (-1)^j \cdot c_{i-jl}.$$

Dann ist

$$A \circ f_k(a) = \tilde{f}_{(k,-k)}(a),$$

wobei $\tilde{f}_{(k,-k)}$ die Trithemius-Belaso-Chiffre zum Schlüssel $(k_0, \ldots, k_{l-1}, -k_0, \ldots, -k_{l-1}) \in \Sigma^{2l}$ ist. *Die Autokey-Chiffre ist also auf die* Trithemius-Belaso-*Chiffre reduzierbar, wobei die Periode die* doppelte *Schlüssellänge ist.* [Friedman und Shannon]