



Bezeichnungen

Sei $\Sigma = \{s_0, \dots, s_{n-1}\}$ das Alphabet.

Der Schlüssel $(\sigma, k) \in \mathbf{S}(\Sigma) \times \Sigma^l$ besteht aus einem (mit σ permutierten) Primäralphabet und einem Kennwort $k = (k_0, \dots, k_{l-1}) \in \Sigma^l$.

Die Verschlüsselungsfunktion wird so bezeichnet:

$$f_{\sigma, k}: \Sigma^* \rightarrow \Sigma^*$$

Spezialfall

$f_{\varepsilon, k}$ ist die BELASO-Chiffre mit Schlüssel k , wenn mit $\varepsilon \in \mathbf{S}(\Sigma)$ die identische Permutation bezeichnet wird.

Die Alphabet-Tafel

... hat dann die Gestalt

$$\begin{array}{cccccc}
 s_0 & s_1 & s_2 & \dots & s_{n-1} & \\
 \hline
 t_0 & t_1 & t_2 & \dots & t_{n-1} & \\
 t_1 & t_2 & t_3 & \dots & t_0 & \\
 \cdot & \cdot & \cdot & \dots & \cdot & \\
 t_{n-1} & t_0 & t_1 & \dots & t_{n-2} &
 \end{array}$$

mit $t_i = \sigma(s_i)$ für $0 \leq i \leq l-1$.

Die Verschlüsselungsfunktion

Wird ein Text $a = (a_0, a_1, a_2, \dots) \in \Sigma^l$ verschlüsselt, so muss man den Geheimtextbuchstaben

$$c_i = t_{p+q} = \sigma(s_{p+q}) = \sigma(s_p + s_q) \quad [\text{Summe in } \mathbf{Z}/n\mathbf{Z}]$$

zum Klartextbuchstaben a_i in Zeile p und Spalte q ablesen mit

$$a_i = s_q, \quad k_i = t_p = \sigma(s_p), \quad s_p = \sigma^{-1}(k_i).$$

Also ist

$$c_i = \sigma(a_i + \sigma^{-1}(k_i)),$$

wobei die Summe in $\mathbf{Z}/n\mathbf{Z}$ zu bilden ist.

Mit dieser Überlegung ist gezeigt, wobei f_σ die monoalphabetische Verschlüsselung zu σ bezeichnet:

Satz. Die PORTA-Chiffre $f_{\sigma,k}$ ist die Komposition (»Überchiffrierung«) der BELASO-Verschlüsselung $f_{\epsilon,k'}$ - wobei $k' = f_\sigma^{-1}(k)$ - mit der monoalphabetischen Verschlüsselung f_σ :

$$f_{\sigma,k} = f_\sigma \circ f_{\epsilon,k'}.$$

Algorithmus

Daraus ergibt sich der folgende Algorithmus:

1. Bilde $k' = f_\sigma^{-1}(k)$, also $k'_i = \sigma^{-1}(k_i)$ für $0 \leq i < l$.
2. Addiere a mit dem periodisch verlängerten k' in $\mathbf{Z}/n\mathbf{Z}$, Ergebnis $b \in \Sigma'$; also $b_j = a_j + k'_j \bmod n$.
3. Bilde $c = f_\sigma(b) \in \Sigma'$; also $c_j = \sigma(b_j)$.

Das entsprechende Perl-Programm steht [hier](#), das passende zur Entschlüsselung [hier](#).

Autor: Klaus Pommerening, 13. November 1999; letzte Änderung: 30. April 2002.

[E-Mail](mailto:Pommerening@imsd.uni-mainz.de) an Pommerening@imsd.uni-mainz.de.