Mathematische Beschreibung eines Rotors

Das Alphabet Σ wird wieder mit **Z**/*n***Z**, den ganzen Zahlen modulo *n* identifiziert.

Sei ρ die monoalphabetische Substitution, die durch die Grundstellung des Rotors bewirkt wird.

In der um eine Stelle rotierten Position (siehe obiges Beispiel) wird dann die Substitution

$$\rho^{(1)}(a) = \rho(a\text{-}1) + 1$$

ausgeführt. [Dies ergibt die Zeile 1 in der Substitutionstabelle.]

Bezeichnet man mit τ die Verschiebung des Standard-Alphabets Σ = **Z**/*n***Z** um 1 (also $\tau(a) = a+1$), so wird die Formel zu

$$\rho^{(1)}(a) = \tau\rho\tau^{-1}(a).$$

Durch Induktion folgt sofort Teil (i) von:

Satz (von den rotierten Alphabeten). (i) *Bewirkt ein Rotor in Grundstellung die Substitution mit dem Primäralphabet* ρ, *so bewirkt er in der um t Stellen rotierten Position die Substitution mit dem Alphabet*

$$\rho^{(t)} = \tau^t\rho\tau^{-t}.$$

Insbesondere sind alle rotierten Alphabete vom gleichen Zykel-Typ.

(ii) *In der zugehörigen polyalphabetischen Substitutionstabelle enthalten die Diagonalen jeweils ein* (*zyklisch fortgesetztes*) *Standard-Alphabet.*

Der *Beweis* von Teil (ii) folgt direkt, wenn man die Aussage als Formel interpretiert:

$$\rho^{(i)}(j) = \tau^i\rho\tau^{-i}(j) = \rho(j\text{-}i) + i = \rho^{(i\text{-}1)}(j\text{-}1) + 1.\blacklozenge$$

Erläuterung zum »*Zykel-Typ*«: Jede Permutation lässt sich, eindeutig bis auf die Reihenfolge, als Produkt von disjunkten Zykeln = zyklischen Permutationen schreiben. Der Zykel-Typ ist das *n*-Tupel

$$(\lambda_1, ..., \lambda_n) \quad \text{mit} \quad \lambda_i = \text{Anzahl der Zykeln der Länge } i,$$

wobei *n* allgemein die Größe der zu permutierenden Menge, bei uns also das Alphabet Σ, ist.

[Insbesondere ist $\lambda_1 + 2\lambda_2 + ... + n\lambda_n = n$.]

Hier gibt's ein Perl-Programm, das eine Ein-Rotor-Chiffre durchführt.

Autor: Klaus Pommerening, 5. Dezember 1999; letzte Änderung: 18. Dezember 1999

E-Mail an Pommerening@imsd.uni-mainz.de.