

Den mathematischen Hintergrund über Permutationen findet man hier als [PDF](#).

Parameter

- Zahl der Buchstaben des Alphabets = $n = \#\Sigma$.
- Zahl der Scheiben = q mit $1 \leq q$;
falls alle Scheiben *verschieden* sein sollen, ist $q \leq (n-1)!$.
[Die Erklärung, warum hier nicht etwa $n!$ steht, folgt unten.]
 - Jede Scheibe ist durch eine Permutation $\tau \in \mathbf{S}(\Sigma)$ gekennzeichnet.
 - Die Menge der Scheiben ist also als Familie (q -Tupel) $(T_1, \dots, T_q) \in \mathbf{S}(\Sigma)^q$ beschreibbar.
(Die Scheiben werden meist mit Nummern versehen; der Schlüssel wird dann durch die entsprechende Nummernfolge beschrieben.)
- Zahl der ausgewählten Scheiben = l mit $1 \leq l \leq q$.
 - Ein Schlüssel ist also eine Folge $(\tau_0, \dots, \tau_{l-1})$ aus verschiedenen Scheiben der Familie (T_1, \dots, T_q) .
 - Es gibt dafür

$$\#K = q \cdot (q-1) \cdots (q-l+1) = q! / (q-l)!$$

Möglichkeiten (von denen einige identisch sein können, falls es gleiche Scheiben gibt).

Beispiele

1. **JEFFERSON**: $l = q = 36$, $\#K = 36!$, effektive Schlüssellänge ≈ 138 .
2. **BAZERIES**: $l = q = 20$, $\#K = 20!$, effektive Schlüssellänge ≈ 61 .
3. **M-94**: $l = q = 25$, $\#K = 25!$, effektive Schlüssellänge ≈ 84 .
4. **M-138-A**: $l = 30$, $q = 100$, $\#K = 100!/70!$, effektive Schlüssellänge ≈ 190 .

Ver- und Entschlüsselung

Die Verschlüsselung ist polyalphabetisch mit der Periode l .

Achtung: Die Scheiben-beschreibende Permutation $\tau \in \mathbf{S}(\Sigma)$ darf nicht mit dem durch die Scheibe definierten Substitutionsalphabet $\sigma \in \mathbf{S}(\Sigma)$ verwechselt werden. Der Zusammenhang zwischen beiden wird gleich erklärt.

Ist das Standard-Alphabet Σ wie so oft mit $\mathbf{Z}/n\mathbf{Z}$ identifiziert, so sieht die Verschlüsselung eines Klartextblocks so aus (bei Verwendung der 1. Generatrix):

$$a_0 \quad \dots \quad a_i \quad \dots \quad a_{l-1}$$

$$\begin{array}{r}
\tau_i(0) \\
\cdots \\
\text{Suche Eintrag } x \text{ mit } \tau_i(x) = a_i \\
\tau_i(x+1) = c_i \text{ zugehöriger Geheimtextbuchstabe} \\
\cdots \\
\tau_i(n-1)
\end{array}$$

wobei die mittlere Spalte $\tau_i(0), \dots, \tau_i(n-1)$ die Beschriftung der Scheibe Nummer i darstellt.

Also ist

$$c_i = \tau_i(x+1) = \tau_i(\tau_i^{-1} a_i + 1),$$

und die zugehörige Entschlüsselungsfunktion wird beschrieben durch

$$a_i = \tau_i(\tau_i^{-1} c_i - 1).$$

Diese Überlegungen werden zusammengefasst zu:

Satz (von der Zylinder-Chiffrierung). *Der Zusammenhang zwischen der Permutation $\tau \in \mathbf{S}(\Sigma)$, die eine Scheibe beschreibt, und der Permutation $\sigma \in \mathbf{S}(\Sigma)$, die die zugehörige Substitution beschreibt, ist*

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

$$\sigma^{-1}(c) = \tau(\tau^{-1} c - 1).$$

Anders ausgedrückt: σ ist eine zyklische Permutation und τ ist die Zykeldarstellung von σ .

Es gibt $(n-1)!$ verschiedene Zyklen der Länge n . Je n Scheibenbeschreibungen $\tau \in \mathbf{S}(\Sigma)$ liefern dieselbe zyklische Permutation $\sigma \in \mathbf{S}(\Sigma)$. Daher die Einschränkung $q \leq (n-1)!$ oben.

Beispiel: Sei $\Sigma = \{A, \dots, Z\}$ und eine Scheibe beschrieben durch

$$\tau = \text{QWERTZUIOPASDFGHJKLYXCVBNM}.$$

Dann ist σ die Permutation

$$\begin{array}{cccccccccccccccccccccccc}
a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\
S & N & V & F & R & G & H & J & O & K & L & Y & Q & M & P & A & W & T & D & Z & I & B & E & C & X & U
\end{array}$$

Autor: [Klaus Pommerening](#), 3. Dezember 1999; letzte Änderung: 9. Januar 2008.