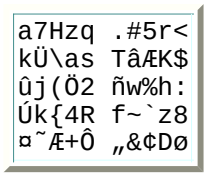
Kryptologie

Transpositions-Chiffren



Allgemeine Definition

Bei Transpositions-Chiffren (deutsche Bezeichnung auch: »Versatzverfahren«) werden die Buchstaben eines Klartextes nicht transformiert, sondern vertauscht (»versetzt«), also permutiert. Dazu gibt es zwei grundsätzliche Möglichkeiten:

1. Aperiodische Transposition: Hier wird ein Text der Länge r einer Permutation der Länge r unterworfen, also einem $\sigma \in \mathbf{S}_r$.
2. Periodische Transposition: Hier wird ein Text beliebiger Länge in Blöcke der Länge l unterteilt - der letzte bei Bedarf mit irgendwelchen Zeichen aufgefüllt - die alle mit der gleichen Permutation $\sigma \in \mathbf{S}_l$ behandelt.

Dabei operiert $\sigma \in \mathbf{S}_l$ auf Σ^l, also auf Texten der Länge l durch die Formel:

$$f_\sigma(a_1, ..., a_l) = (a_{\sigma^{-1}(1)}, ... a_{\sigma^{-1}(l)}).$$

D. h., a_i wird an die Stelle $\sigma(i)$ versetzt.

Beispiel: $l = 5$, $\sigma = (4\ 1\ 5\ 2\ 3)$. Dann ist $\sigma(1) = 4$ usw., also

$$f_\sigma(\text{APFEL}) = \text{PELAF}.$$

Eigenschaften

\+ Der Text wird durchmischt - Muster werden zerrissen.
\+ Die kryptoanalytische Lösung ist im allgemeinen nicht eindeutig: Anagramme.
\- Zeichenhäufigkeiten und Koinzidenzindex sind invariant.
\- Daran ist der Typ der Chiffre leicht erkennbar.

Für eine ausführlichere Behandlung von Transpositions-Chiffren einschließlich ihrer Kryptoanalyse sind die Bücher von Bauer, Gaines, Sinkov und Nichols (Vol. II) zu empfehlen, siehe das Literaturverzeichnis.

Autor: Klaus Pommerening, 21. Januar 2000; letzte Änderung: 16. Januar 2005.