Kryptologie

Transpositions-Chiffren - Beispiele

```
a7Hzq .#5r<
kÜ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

A. Geometrische Transpositionen

Hier wird der Klartext in einer bestimmten Reihenfolge aufgeschrieben und in einer anderen Reihenfolge abgelesen. Die Transposition ist meist auf die Länge des Textes abgestimmt, also aperiodisch.

Beispiel 1: Die Skytale

... (σκυταλε, Briefstab) wurde im alten Griechenland von den Spartanern verwendet. Ein Lederband wird um einen Stab gewunden und in Richtung des Stabes beschrieben. Auf dem abgewickelten Lederband sind die Buchstaben permutiert [Bildchen, Bild].

Beispiel 2: Die Spaltentransposition

[Deutsche historische Bezeichnung: Würfel]

Hier wird der Text in Zeilen der Breite *l* geschrieben und spaltenweise ausgelesen. Und zwar werden die Spalten in einer Reihenfolge ausgelesen die durch den Schlüssel definiert wird. [Werden die Spalten in der natürlichen Reihenfolge ausgelesen, also ohne Verwendung eines Schlüssels, so kann man das Verfahren auch als geometrische Transposition deuten; die Skytale entspricht einer solchen Spaltentransposition mit einem trivialen Schlüssel.]

Beispiel: $l = 5$,

```
Schlüssel = 4 1 5 2 3

Klartext  = A L L E M
            E I N E E
            N T C H E
            N S C H W
            I M M E N
            A U F D E
            M S E E
```

Geheimtext: `LITSMUS EEHHEDE MEEWNE AENNIAM LNCCMFE`, den man dann natürlich wieder in Fünfergruppen umschreibt:

```
LITSM USEEH HEDEM EEWNE AENNI AMLNC CMFE
```

Der berechtigte Empfänger der Nachricht, der den Schlüssel ja kennt, berechnet zuerst die Spaltenlänge, indem er r/l zur nächsten ganzen Zahl aufrundet, und schreibt dann den Geheimtext Spalte für Spalte nach der Ordnung, die der Schlüssel vorgibt. Dabei werden r mod l Spalten vollständig gefüllt, bei den übrigen wird die letzte Stelle frei gelassen.

Der Schlüssel wird hier meist nicht als Zahlenfolge, sondern als **Merkwort** vereinbart. Die Zahlenfolge ist wird dann aus der alphabetischen Ordnung der Buchstaben des Merkworts

hergeleitet, wobei bei gleichen Buchstaben der erste die niedrigere Nummer bekommt. Beispiel:

```
Merkwort  = F A R A D
Schlüssel = 4 1 5 2 3
```

Die Größe des Schlüsselraums für Spaltentranspositionen der Breite *l* ist offensichtlich *l*!.

Bei der *doppelten* Spaltentransposition wird das Verfahren wiederholt - möglicherweise, aber nicht notwendig - mit einer anderen Spaltenbreite und einem anderen Schlüssel. Die doppelte Spaltentranspostion (»Doppelwürfel-Verfahren«) wurde noch im 1. und sogar noch im 2. Weltkrieg eingesetzt und meistens vom jeweiligen Gegner gebrochen; das ist aber schon ziemlich schwierig.

Beispiel 3: Wegtranspositionen

Hier wird der Klartext auf einem ganz bestimmten Weg, z. B. in eine Spirale, geschrieben und dann zeilenweise ausgelesen.

B. Raster-Transpositionen

... sind periodisch. Einfache Raster wurden schon von Ibn AD-DURAIHIM im 14. und von Gerolamo CARDANO im 16. Jahrhundert verwendet; diese ergeben allerdings keine Transposition, sondern sind den steganographischen Methoden zuzurechnen. Drehraster dagegen beschreiben Transpositionen; in dieser Form wurden sie schon im 18. Jahrhundert eingesetzt. Gegen Ende des 19. Jahrhunderts kamen sie etwas in Mode. Für die Beschreibung sei auf den Artikel

> F. L. Bauer: Fleissner-Raster und der Erzherzog, Informatik-Spektrum 30 (2007), 36-38,

sowie den Auszug aus dem Roman »Mathias Sandorf« von Jules Verne verwiesen, insbesondere das vierte Kapitel und den Kommentar.

Im Gegensatz zur dortigen Behauptung ist die Konstruktion eines Drehrasters allerdings sehr leicht: Für eine ganze Zahl l zeichnet man ein 2*l*×2*l*-Quadrat und unterteilt es in vier *l*×*l*-Quadrate.

1	...	*l*		...	1
|		|	|		|
	...	l^2	l^2	...	*l*
l	...	l^2	l^2	...	
|		|	|		|
1	...		*l*	...	1

Im ersten Quadrat nummeriert man die Felder von 1 bis l^2 und überträgt diese Nummerierung rotationssymmetrisch auf die anderen Teilquadrate, wie in der obigen Skizze angedeutet.

Ein Schlüssel besteht dann einfach aus einer Auswahl von je einer der vierfach vorkommenden Zahlen 1 bis l^2 - an diesen Stellen wird dann das Raster mit Öffnungen versehen.

Die Größe des Schlüsselraums ist also 4^{l^2}. Für kleine l ist das:

Parameter *l*:	3	4	5	6
# Schlüssel:	2^{18}	2^{32}	2^{50}	2^{72}

Ab $l = 6$ ist der Schlüsselraum also durchaus ausreichend groß; das macht die Chiffre aber nicht wirklich sicher.

Eine Mischung aus Spalten- und Raster-Transposition wurde noch im zweiten Weltkrieg gelegentlich verwendet (Wehrmacht-Rasterschlüssel 44 und Varianten oder »Kreuzworträtsel-Chiffre«). Hier wurde das Raster aufgelegt und der Klartext zeilenweise in die Ausschnitte geschrieben oder das Raster auf einem Blatt Papier vorgedruckt und ausgefüllt. Z. T. waren einige Ausschnitte für Füllzeichen reserviert und entsprechend markiert. Wurde der Text dann spaltenweise ausgelesen, war er recht willkürlich permutiert.

C. Block-Transpositionen

... sind die allgemeinen periodischen Transpositionen. Für die Blocklänge l gibt es $l!$ verschiedene Schlüssel.

[Deutsche historische Bezeichnung: Umstellung]

Ein Perl-Programm, das Spalten- und Blocktranspositionen ausführt, steht hier.

Autor: Klaus Pommerening, 21. Januar 2000; letzte Änderung: 17. August 2008.