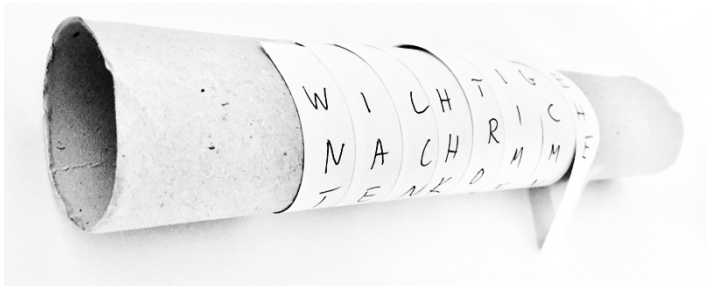
Skytale[1]



- Ca. 2500 Jahre alt, Benutzung durch die Regierung von Sparta.
- Sender und Empfänger müssen beide eine Skytala haben – ein Zylinder mit genau dem gleichen Umfang.
- Der Sender wickelt ein schmales Band spiralförmig um den Zylinder und schreibt der Länge nach seine Nachricht auf das Band.
- Das abgewickelte Papierband enthält nun zwar alle Buchstaben der Nachricht, aber in einer anderen Anordnung. Der Klartext ist verschoben (Verschiebung = **Transposition**)
- Der Empfänger wickelt das Papierband um einen Zylinder mit gleichem Umfang und kann die Nachricht jetzt lesen.
- Das Verfahren zur Chiffrierung ist somit, den Text spaltenweise (von oben nach unten) mit einer bestimmten Anzahl von Zeilen aufzuschreiben. Die Anzahl der Windungen (=Anzahl der Buchstaben, die in einer Zeile stehen) bestimmt die Anordnung des Textes und dient somit als **Schlüsselzahl**.
- Häufig findet man in der Literatur den Hinweis, dass der *Umfang* des Zylinders für die Ver- und Entschlüsselung angegeben werden muss. Dabei ist die Anzahl der Buchstaben gemeint, die benötigt wird, um einmal um den Zylinder herum zu schreiben. Dies entspricht der Anzahl der Zeilen. In unserem Beispiel erkennt man gut, dass der Streifen (linker Rand der Seite) Lücken enthält, wenn die Skytale nicht vollgeschrieben wurden. Das vereinfacht die Entschlüsselung erheblich. Denn jetzt brauchen die einzelnen Blöcke nur nebeneinander geschrieben zu werden.

Beispiel

Verschlüsselung (Chiffrierung)

Klartext (31 Zeichen): WICHTIGENACHRICHTENKOMMENMORGEN

Im Beispiel haben wir **8** Windungen (Schlüsselzahl) des Bandes. Das bedeutet wir benötigen eine Tabelle mit 8 Spalten und ((31 DIV[2] 8) + 1) = 4 Zeilen[3]. Hinweis. Man kann bei diesem Verfahren einfach in der ersten Zeile beginnen und mit dem Text die Tabelle füllen, ohne die genaue Anzahl der Zeilen zu kennen. Die Zeilenanzahl ist für das Verständnis wichtig und für die Entschlüsselung (vgl. unten).

Dann tragen wir den Text wie auf einer Skytale ein:

W	I	C	H	T	I	G	E
N	A	C	H	R	I	C	H
T	E	N	K	O	M	M	E
N	M	O	R	G	E	N	

Jetzt wird der Text spaltenweise (von oben nach unten) aus der Tabelle ausgelesen:

Geheimtext: WNTNIAEMCCNOHHKRTROGIIMEGCMEEHE

Entschlüsselung (Dechiffrierung)

Wenn man die **Schlüsselzahl** kennt (hier 8) kann man aus der Länge der Nachricht die benötigte Anzahl von Zeilen ermitteln (hier 4). Dann lässt sich die Tabelle wieder spaltenweise (von oben nach unten) mit dem **Geheimtext** füllen. In den Zeilen lässt sich der Klartext ablesen (vgl. Tabelle oben).

Hinweis: Meist ist die Schlüsselzahl (Anzahl der Windungen) nicht bekannt und es muss mit verschiedenen Ansätzen experimentiert werden.

Beispiel für die **Vermutung** Schlüsselzahl = 4. Dann beträgt die Anzahl der Zeilen 8 (warum?)

W	C	T	
N	C	R	
T	N	O	
N	O		
I	H		
A	H		
E	K		
M	R		

Auch ohne die Tabelle vollständig ausgefüllt zu haben, lässt sich schnell erkennen, dass die Nachricht kein sinnvoller Text sein kann: „WCTNCRTNO...“

[1] Bild von F.Oppermann, Text nach A. Beutelspacher: Kryptologie. 9. Auflage, S. 3ff.

[2] DIV bedeutet hier die ganzzahlige Division ohne Nachkommastellen

[3] +1 deshalb, da 31 DIV 8 = 3 REST 7 ist. Deshalb benötigen wir 1 Zeile mehr, davon werden die 7 ersten Spalten belegt.