

Transposition

Verschlüsseln von Texten ist mit vielen verschiedenen Verfahren möglich. Einige dieser Verfahren lassen sich durch dem Begriff *Transposition* beschreiben. Bei der Transposition werden (meist) Buchstaben des Klartextes so verschoben, dass die eigentlich Nachricht nicht mehr direkt lesbar ist. Dabei kann es vorkommen, dass zusätzliche Gegenstände zum Entschlüsseln notwendig sind (siehe Skytale), dies ist aber nicht zwingend der Fall (siehe fleißnersche Schablone, Gartenzaun oder Krebs-Verfahren).

Skytale-Verschlüsselung

Bei der Skytale-Verschlüsselung wird ein Holzstab (der sogenannte Skytale) mit einem bestimmten Durchmesser verwendet. Um diesen Holzstab wird dann das Papier (oder damals Leder) herumgewickelt und darauf geschrieben (siehe rechtes Bild). Der Durchmesser ist der Schlüssel.



Aufgabe 1

Verschlüsse die folgende Nachricht mit einer der bereitgestellten Skytales:




Austausch heute Abend am bekannten Ort

Aufgabe 2

Suche dir eine Partnerin oder einen Partner und verschlüsselt jeweils eine Nachricht mit einen der bereitgestellten Skytales.

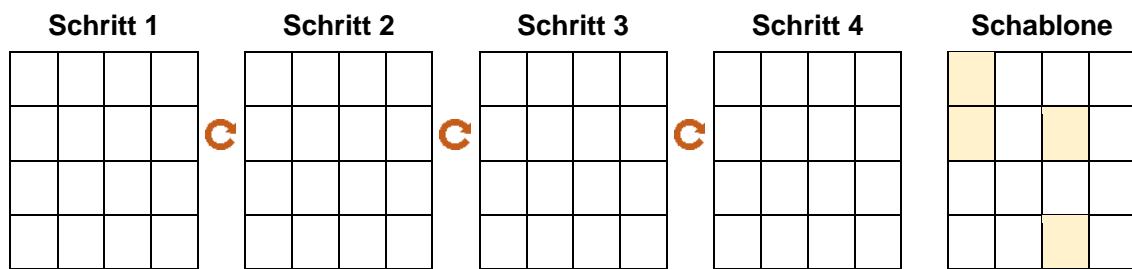
Verschlüsselung mittels fleißnersche Schablone

Ein anderes Hilfsmittel stellt die fleißnersche Schablone dar (die nicht zwingend physisch vorhanden sein muss). Der Klartext wird hier in eine Art Tabelle bzw. Matrix geschrieben, wobei eine Schablone vorgibt, wo etwas eingetragen werden darf. Sind alle erlaubten Felder genutzt, wird die Schablone mit oder gegen den Uhrzeigersinn (aber immer einheitlich) gedreht und der verbleibende Text mittels Schablone eingetragen. Das folgende Beispiel zeigt wie der Text „Ich mag Informatik“ verschlüsselt wird. Die gelben Kästchen geben die erlaubten Felder der Schablone an.

Schritt 1		Schritt 2		Schritt 3		Schritt 4		Schablone																																																																											
<table><tr><td>I</td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td>C</td><td></td><td>H</td></tr><tr><td></td><td>M</td><td></td></tr></table>	I						C		H		M			<table><tr><td>I</td><td>A</td><td></td><td>G</td></tr><tr><td>I</td><td></td><td></td><td></td></tr><tr><td>C</td><td>N</td><td>H</td><td></td></tr><tr><td></td><td>M</td><td></td><td></td></tr></table>	I	A		G	I				C	N	H			M				<table><tr><td>I</td><td>A</td><td>F</td><td>G</td></tr><tr><td>I</td><td>O</td><td></td><td>R</td></tr><tr><td>C</td><td>N</td><td>H</td><td></td></tr><tr><td></td><td>M</td><td></td><td>M</td></tr></table>	I	A	F	G	I	O		R	C	N	H			M		M		<table><tr><td>I</td><td>A</td><td>F</td><td>G</td></tr><tr><td>I</td><td>O</td><td>A</td><td>R</td></tr><tr><td>C</td><td>N</td><td>H</td><td>T</td></tr><tr><td>I</td><td>M</td><td>G</td><td>M</td></tr></table>	I	A	F	G	I	O	A	R	C	N	H	T	I	M	G	M	<table><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table>																
I																																																																																			
C		H																																																																																	
	M																																																																																		
I	A		G																																																																																
I																																																																																			
C	N	H																																																																																	
	M																																																																																		
I	A	F	G																																																																																
I	O		R																																																																																
C	N	H																																																																																	
	M		M																																																																																
I	A	F	G																																																																																
I	O	A	R																																																																																
C	N	H	T																																																																																
I	M	G	M																																																																																

Aufgabe 3

Verschlüsse einen Satz mittels fleißnerscher Schablone.



Aufgabe 4

Entschlüsse die folgende Nachricht.

Nachricht				Schablone			
B	R	H	T				
R	H	C	E				
A	I	K	U				
A	M	U	M				