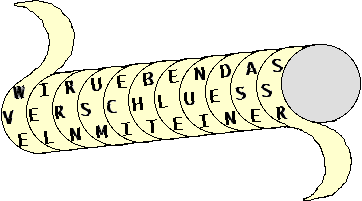
## Die Spartanische Skytale

Der griechische Historiker Plutarch sagt uns, dass die Spartanische Regierung (etwa 500 v. Chr.) Nachrichten an ihre Generäle folgendermaßen verschlüsselte:  
Man wickelte einen schmalen Pergamentstreifen um einen Zylinder und schrieb die Nachricht längsseits auf den Streifen; anschließend wickelte man den Streifen wieder ab und schickte ihn per Boten zum Empfänger. Dieser brauchte, um die Nachricht lesen zu können, einen Zylinder mit gleichem Umfang bzw. Radius (griech. Skytale, skutalh). Bei dieser Skytale-Methode werden keine geheimen Zeichen oder Zahlen benutzt. Die Buchstaben bleiben, was sie sind, aber sie verändern ihren Platz.



Sie bleiben was sie sind, aber nicht wo sie sind. Man spricht von **Transposition**.

## Beispiele zur Skytale

1. Verwendung von fertig verschlüsselten Nachrichten  
      
   Beispiel A

|  |
| --- |
| mrrriearoocristdhssasnherokaresnirbiwflsdkestaefaoasiltpisgt |

Beispiel B

|  |
| --- |
| fcdnthatsuegueuauhiiadnvcellbsr!etccuunehsnaenj!rehhcksrls |

Beispiel C

|  |
| --- |
| nuirlserensfkpwutmsueigibctltirbvcelnemoheagsmeehsnehetaspes |

**Aufgabe 1: Kannst du diese Nachricht entschlüsseln?**

* + Was wäre für dich hilfreich beim Entschlüsseln?
  + Tipp: Schreibe die Buchstaben auf einen schmalen Steifen kariertes Papier, Kästchen für Kästchen untereinander
  + Wickele das schmale Papierband um einen passenden Zylinder (Experimentieren - Radius etwa 1 cm).

1. Herstellen eigener verschlüsselter Nachrichten  
     
   **Aufgabe 2: Stelle selbst eine verschlüsselte Botschaft her.** 
   * Wickele dazu einen schmalen Streifen Karopapier um einen Zylinder z.B. PRITT®-Klebestift.
   * Beschrifte den Streifen dann längsseits mit deiner Geheimbotschaft (kurzer sinnvoller Satz).
   * Lass deinen Nachbarn die Botschaft entschlüsseln.

## Weitere Beispiele für eine Entschlüsselung mittels Transposition

Wenn man keinen Zylinder passenden Umfangs zur Verfügung hat, kann man zum Entschlüsseln auch versuchen, den Umfang der Skytale durch eine bestimmte Anzahl n von Buchstaben zu ersetzen.  
Für n = 12 ergibt sich, Spalte für Spalte notiert, bei Beispiel A eine Darstellung wie in Bild 1.  
Für andere Längen z.B. n = 6 ergibt sich kein sinnvoller Text, vgl. Bild 2.

Ein weiteres Beispiel einer verschlüsselten Nachricht, zum Entschlüsseln spaltenweise notiert für n = 6, zeigt Bild 3.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | Bild 1 | | |  |  |  |  |  | | --- | --- | --- | --- | --- | | m | i | r | w | a | | r | s | o | f | o | | r | t | k | l | a | | r | d | a | s | s | | i | h | r | d | i | | e | s | e | k | l | | a | s | s | e | t | | r | a | n | s | p | | o | s | i | t | i | | o | n | r | a | s | | c | h | b | e | g | | r | e | i | f | t | | | |  | | --- | | Bild 2 | | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | m | a | i | s | r | s | w | e | a | t | | r | r | s | a | o | n | f | s | o | p | | r | o | t | s | k | i | l | t | a | i | | r | o | d | n | a | r | s | a | s | s | | i | c | h | h | r | b | d | e | i | g | | e | r | s | e | e | i | k | f | l | t | | | Bild 3 | | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | s | i | c | h | e | r | h | e | | i | t | i | s | t | e | i | n | | w | i | c | h | t | i | g | e | | s | z | i | e | l | d | e | r | | k | r | y | p | t | o | g | r | | a | p | h | i | e | ! |  |  | | |

## Transposition ohne Skytale - Zerlegung mit Rest

Wir versuchen, einen Text mittels Skytalemethode zu verschlüsseln, indem wir den Umfang der Skytale durch eine bestimmte Anzahl n von Buchstaben angeben. Wir wählen denselben Klartext und verschlüsseln ihn auf verschiedene Weisen.

Der zu verschlüsselnde Text umfasst 44 Zeichen und lautet:

|  |
| --- |
| miteinerskytaleverschluesselnwillgelerntsein |

1. Zerlegung: 44 = 4 · 11 + 0  
   Diese Zerlegung gibt an, dass man den Text in 4 Zeilen zu je 11 Zeichen unterbringen kann.  
   n = 4

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| m | i | t | e | i | n | e | r | s | k | y |
| t | a | l | e | v | e | r | s | c | h | l |
| u | e | s | s | e | l | n | w | i | l | l |
| g | e | l | e | r | n | t | s | e | i | n |

Dann lautet der verschlüsselte Text

|  |
| --- |
| MTUGIAEETLSLEESEIVERNELNERNTRSWSSCIEKHLIYLLN |

1. Zerlegung: 44 = 5 · 8 + 4 = 6 · 8 - 4  
   Diese Zerlegung gibt an, dass man den Text in 5 Zeilen zu je 8 Zeichen unterbringen kann und eine zusätzliche Zeile mit 4 Zeichen anhängen muss; insgesamt sind also 6 Zeilen zu notieren, wobei in der letzten Zeile 4 Zeichen fehlen.   
   n = 6

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| m | i | t | e | i | n | e | r |
| s | k | y | t | a | l | e | v |
| e | r | s | c | h | l | u | e |
| s | s | e | l | n | w | i | l |
| l | g | e | l | e | r | n | t |
| s | e | i | n |  |  |  |  |

Dann lautet der verschlüsselte Text

|  |
| --- |
| MSESLSIKRSGETYSEEIETCLLNIAHNE NLLWR EEUIN RLEVT |

Diese Variante ist schlecht, weil aus der großen Anzahl von Lücken im Geheimtext Rückschlüsse auf n = 6 möglich sind.

1. Zerlegung: 44 = 8 · 5 + 4 = 9 · 5 - 1  
   Diese Zerlegung gibt an, dass man den Text in 8 Zeilen zu je 5 Zeichen unterbringen kann und eine zusätzliche Zeile mit 4 Zeichen anhängen muss; insgesamt sind also 9 Zeilen zu notieren, wobei in der letzten Zeile 1 Zeichen fehlt.  
   n = 9

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| m | i | t | e | i |
| n | e | r | s | k |
| y | t | a | l | e |
| v | e | r | s | c |
| h | l | u | e | s |
| s | e | l | n | w |
| i | l | l | g | e |
| l | e | r | n | t |
| s | e | i | n |  |

Dann lautet der verschlüsselte Text

|  |
| --- |
| MNYVHSILSIETELELEETRARULLRIESLSENGNNIKECSWET |