

# Scytale

The Spartan *scytale* dates back to ca. 500 B.C., making it one of the earliest encryption devices known. It was used by the Spartan Military for encoding messages sent between commanders. The scytale consisted of a ribbon wrapped around a dowel of a particular diameter and length. The secret message was written left to right on the ribbon when it was wrapped around the dowel. The ribbon was then removed from the dowel, and only the ribbon was transported to the other field commander who had an identical dowel that could be used to decode the message. If the ribbon was intercepted, it is seemingly contained just a jumble of letters.



Scytale

The following example illustrates how the scytale works. Assume we are working with a dowel having a diameter allowing to write four letters on the ribbon before it wraps again around the dowel. If we want to encode the message "Help me I am under attack", the entire text can be written over seven columns (of which the last three do not use one of the positions). Encoding the text comes down to writing the text from left to right, and from top to bottom on the ribbon.

```
-----+---+---+---+---+---+---+---+---+---+-----
| H | e | l | p | | m | e | * |
+---+ | l | | a | m | | u | * |
| * | n | d | e | r | | a | t | ---+
| * | t | a | c | k | * | * | * |
-----+---+---+---+---+---+---+---+---+---+-----
```

After the ribbon has been released from the dowel, the encoded message reads as "H nteldal ecpark m m aeut". This indeed has turned the message into an incomprehensible series of letters. To decode the text, the ribbon can be wrapped again around a dowel with the same diameter, after which the original text can be read from left to right, and top to bottom.

## Assignment

- Write a function `encode` that takes two arguments: *i*) a text that must be encoded and *ii*) the number of letters that fit on a single wrap of the ribbon around the dowel. The function must return a string containing the encoded message for the given text according to the scytale coding scheme. In coding the text, the minimum number of columns needed to fit the text must be used.
- Write a function `decode` that takes two arguments: *i*) a text encoded according to the scytale coding scheme and *ii*) the number of letters that fits on a single wrap of the ribbon around the dowel. The function must return a string containing the original text after decoding.

## Example

```
>>> encode('Help me I am under attack', 4)
'H nteldal ecpark m m aeut'
```

```
>>> decode('H nteldal ecpark m m aeut', 4)
'Help me I am under attack'
```

```
>>> encode('Always look on the bright side of life.', 7)
'A o t fllnb oewo rsf.aotii ykhgdls ehei'
```

```
>>> decode('A o t fllnb oewo rsf.aotii ykhgdls ehei', 7)
'Always look on the bright side of life.'
```

De Spartaanse *scytale* dateert van ca. 500 voor Christus, en is daarmee één van de oudste coderingsinstrumenten. Ze werd gebruikt door het Spartaanse leger om gecodeerde boodschappen te verzenden tussen bevelhebbers. De scytale bestond uit een houten stok van een bepaalde diameter en lengte, waarrond een lederen riem werd gewikkeld. De geheime boodschap werd van links naar rechts op de riem geschreven terwijl die rond de houten stok gewikkeld zat. Vervolgens werd de riem van de stok verwijderd en afzonderlijk van de stok naar een bevelhebber gestuurd. Deze gebruikte dan een houten stok met dezelfde afmetingen om de boodschap te decoderen. Wanneer enkel de riem werd onderschept, leek die alleen maar een onsamenhangende wirwar van letters te bevatten.



Scytale

Het volgende voorbeeld illustreert de werking van de scytale. Veronderstel dat we werken met een houten stok die ons toelaat om vier letters op de riem te schrijven vooraleer die een volgende keer rond de stok gewikkeld wordt. Als we de boodschap "Help me I am under attack" willen coderen, dan kunnen we de volledige tekst dus vatten in zeven kolommen (waarvan de laatste drie kolommen telkens een positie onbenut laten). Om de tekst te coderen, wordt deze van links naar rechts, en van boven naar onder op de lederen riem geschreven.

```
-----+--+--+--+--+--+--+--+--+--+
|H|e|l|p| |m|e|*|
+---| |l| |a|m| |u|*|
|*|n|d|e|r| |a|t|---+
|*|t|a|c|k|*|*|*|
-----+--+--+--+--+--+--+--+-----
```

Nadat de lederen riem van de stok werd gewikkeld, leest de gecodeerde boodschap als "H nteldal ecpark m m aeut". Daar valt inderdaad kop nog staart aan te krijgen. Om de boodschap te decoderen volstaat het om de lederen riem rond een stok met dezelfde afmetingen te wikkelen, en daarna de tekst terug van links naar rechts en van boven naar onder af te lezen. Het is echter een ander paar mouwen om dat coderen en decoderen aan een computer uitgelegd te krijgen.

## Opgave

- Schrijf een functie `codeer` waaraan twee argumenten moeten doorgegeven worden: *i*) een tekst die moet gecodeerd worden en *ii*) het aantal letters dat op één enkele wikkel van de lederen riem past wanneer die rond de houten stok wordt gewikkeld. De functie moet als resultaat een string teruggeven, die de gecodeerde versie van de gegeven tekst bevat volgens de scytale codering. Bij het coderen moeten zo weinig mogelijk kolommen gebruikt worden.
- Schrijf een functie `decodeer` waaraan twee argumenten moeten doorgegeven worden: *i*) een tekst die gecodeerd werd volgens de scytale codering en *ii*) het aantal letters dat op één enkele wikkel van de lederen riem past wanneer die rond de houten stok wordt gewikkeld. De functie moet als resultaat een string teruggeven die de originele tekst na decodering bevat.

## Voorbeeld

```
>>> codeer('Help me I am under attack', 4)
'H nteldal ecpark m m aeut'
```

```
>>> decodeer('H nteldal ecpark m m aeut', 4)
'Help me I am under attack'
```

```
>>> codeer('Always look on the bright side of life.', 7)
'A o t flnb oewo rsf.aotii ykhgdls ehei'
```

```
>>> decodeer('A o t flnb oewo rsf.aotii ykhgdls ehei', 7)
'Always look on the bright side of life.'
```