

# Die Cäsar-Verschlüsselung

## Historisches

- Namensgeber: Julius Gaius **Cäsar**, 100-44 v. Chr.
- Verschlüsselte Kommunikation für militärische Zwecke



## Die Cäsar-Verschlüsselung

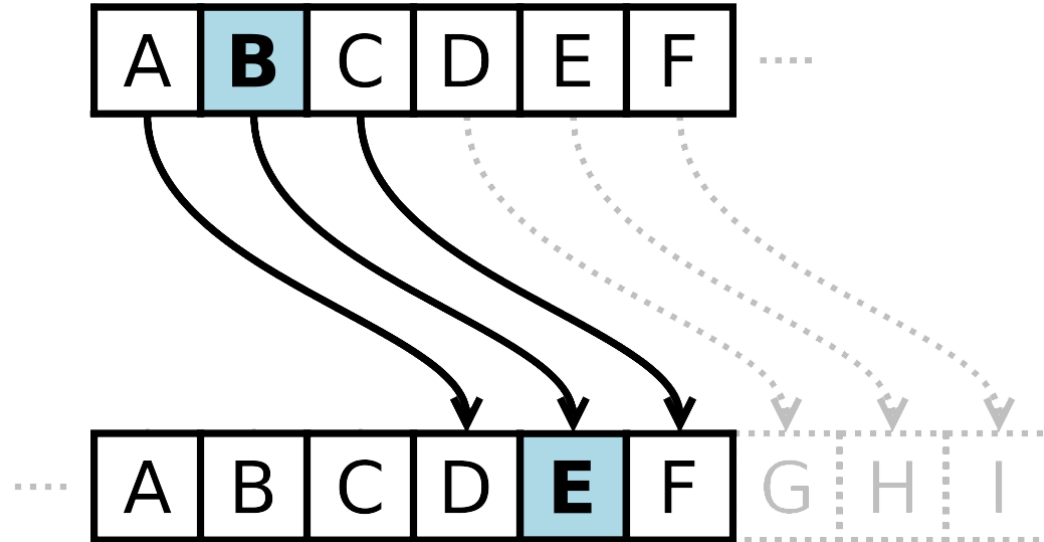
### Voraussetzung:

- Buchstaben aus dem lateinischen Alphabet
- Sender und Empfänger haben gleichen Schlüssel

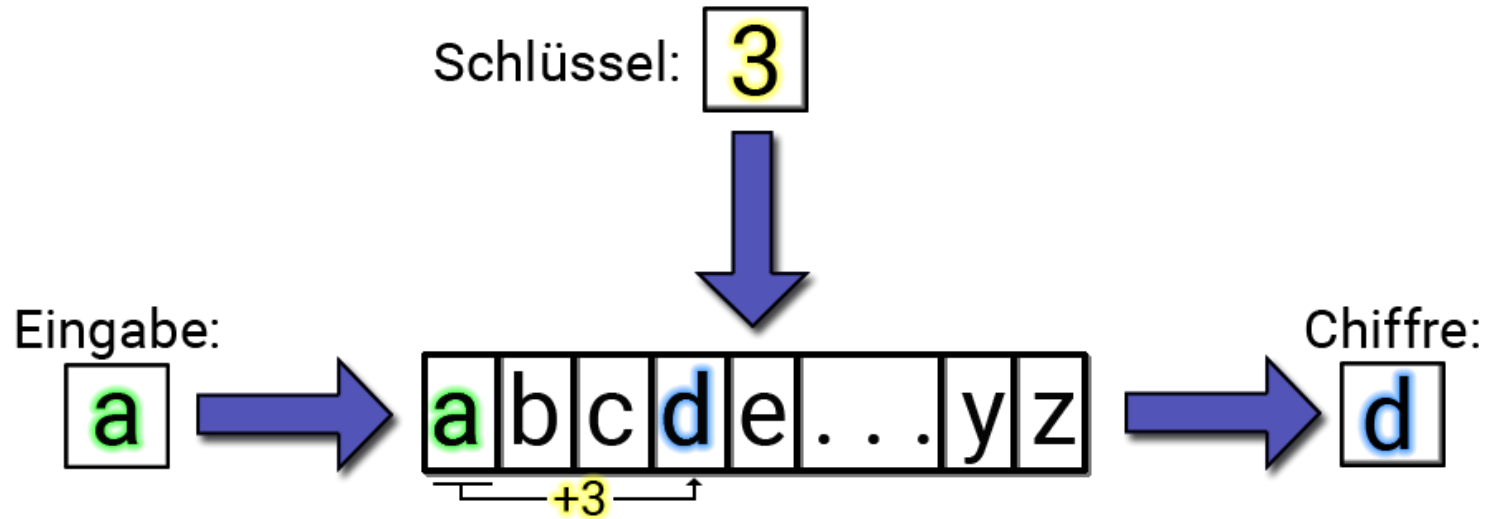
### Vorgehen:

- Jeder einzelne Nachrichten-Buchstabe wird durch einen bestimmten Anderen ersetzt.
- Durch welchen bestimmt der **Schlüssel**.

## Was macht die Cäsar-Verschlüsselung?

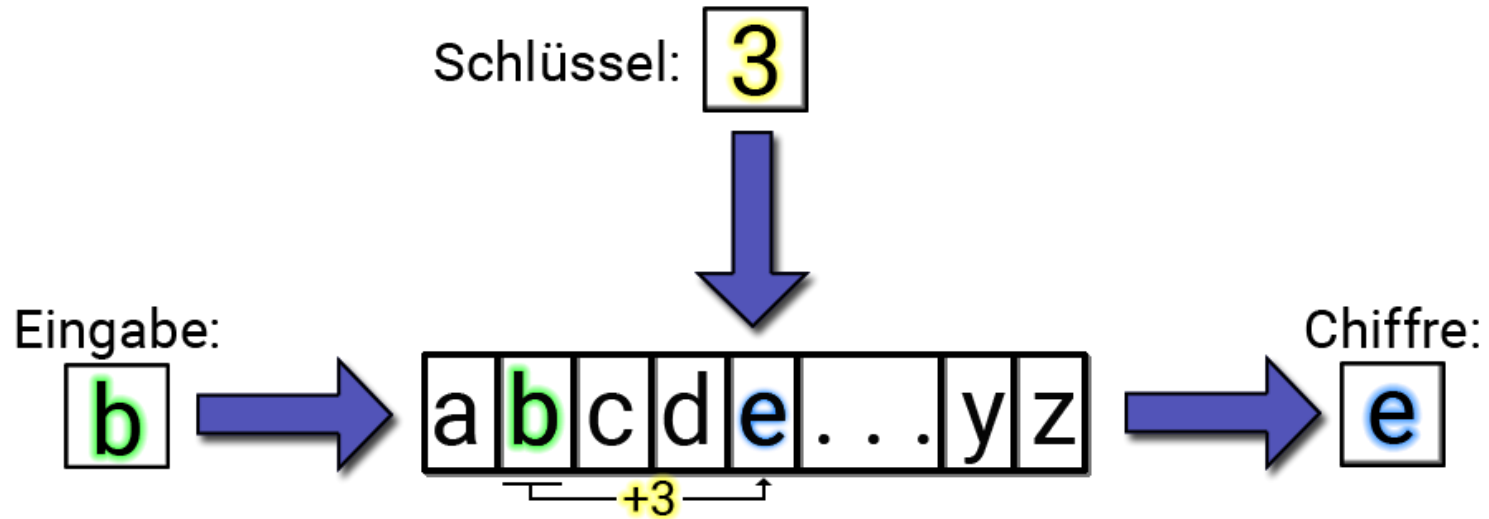


## Verschlüsseln mit dem Schlüsselwert 3



Verschiebung des Buchstabens „a“ um den Schlüsselwert 3

## Verschlüsseln mit dem Schlüsselwert 3



Verschiebung des Buchstabens „b“ um den Schlüsselwert 3



## Auftrag Nr.1

Wende die Verschiebung um 3 Positionen auf die Nachricht „Julius“ an.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**Chiffre:** „mxolxv“

## Wie hat Cäsar Nachrichten verschlüsselt?

Cäsar verwendete den Schlüsselwert 3, wir können aber auch jede andere (ganze) Zahl verwenden!



## Auftrag Nr.2

Wende die Verschiebung um 5 Positionen auf die Nachricht „Julius“ an.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

**Chiffre:** „ ozqnzx“



## Die Cäsar-Verschlüsselung

### Vorschrift:

- Jeder Buchstabe wird durch den Buchstaben ersetzt, der eine bestimmte Anzahl an Stellen rechts von ihm steht.
- Der **Schlüssel** ist die Anzahl der Stellen.



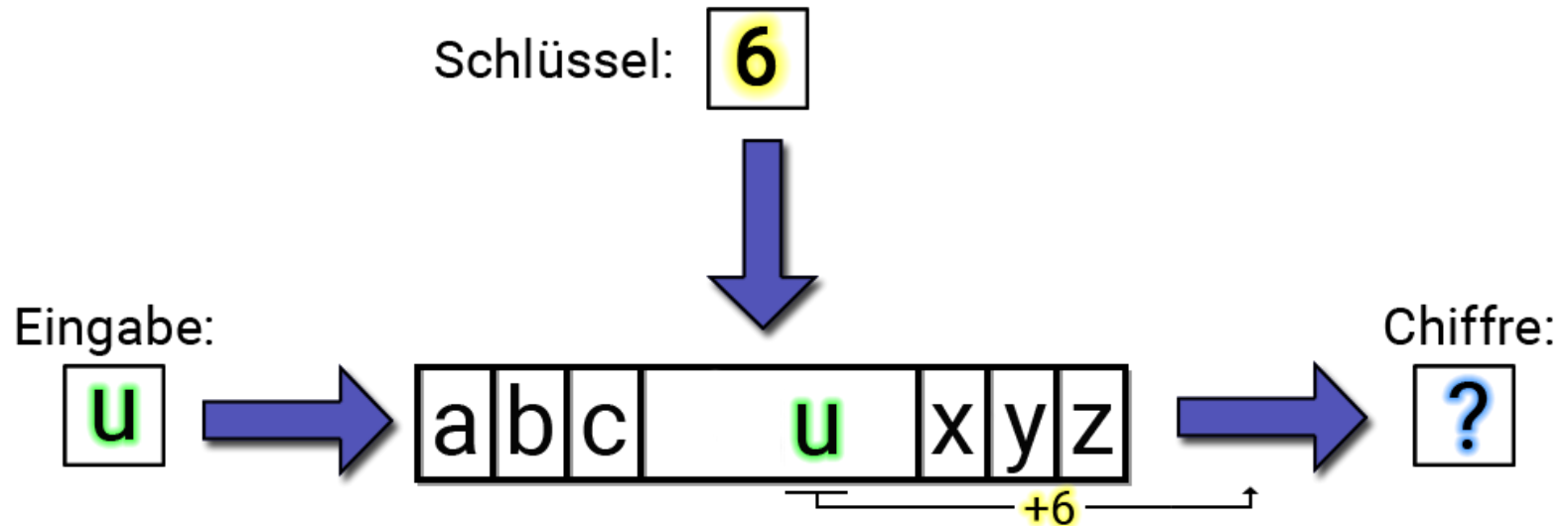
## Auftrag Nr.3

Wende die Verschiebung um 6 Positionen auf die Nachricht „Julius“ an.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Chiffre: „p?ro?y “

# Verschlüsseln



Verschiebung des Buchstabens „u“ um den Schlüsselwert 6



## Die Cäsar-Verschlüsselung

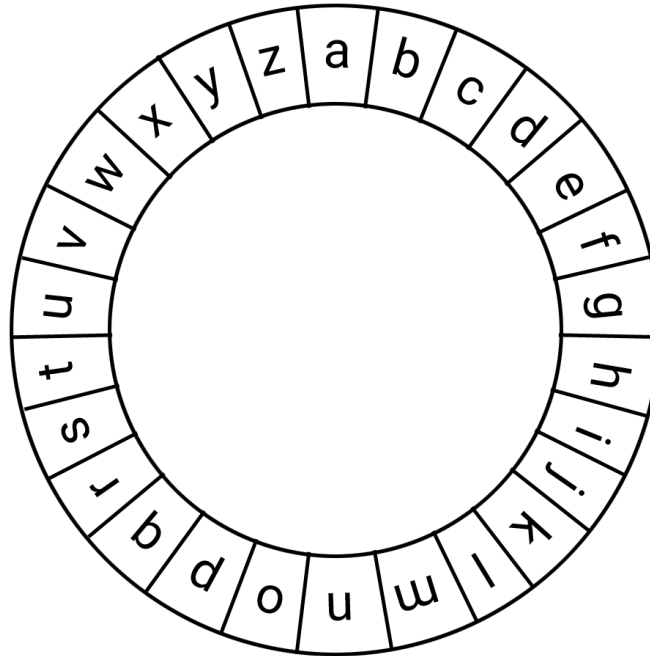
### Vorschrift:

- Jeder Buchstabe wird durch den Buchstaben ersetzt, der eine bestimmte Anzahl an Stellen rechts von ihm steht.
- Der **Schlüssel** ist die Anzahl der Stellen.
- Müssen wir über das „z“ hinaus schieben, beginnen wir wieder von Vorne.

## Vorstellung, beim „über das z Hinausschieben“

|     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |     |
|-----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----|
| ... | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | ... |
|-----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|-----|

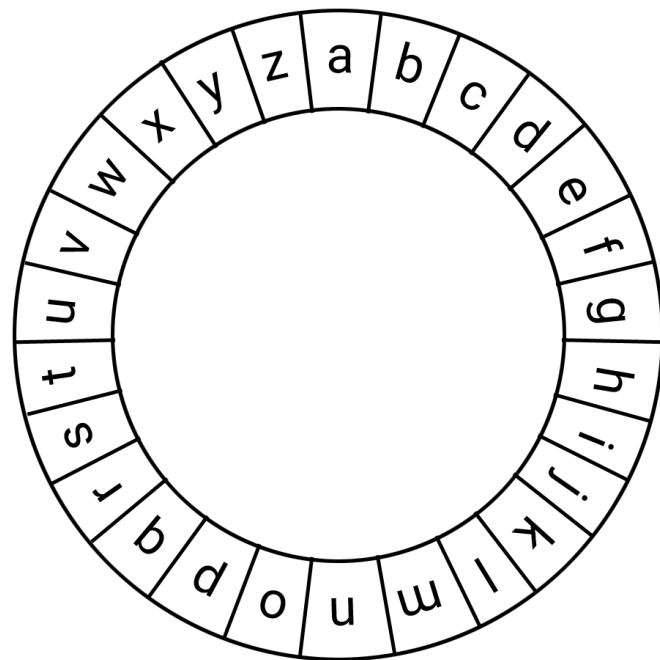
## Vorstellung, beim „über das z Hinausschieben“



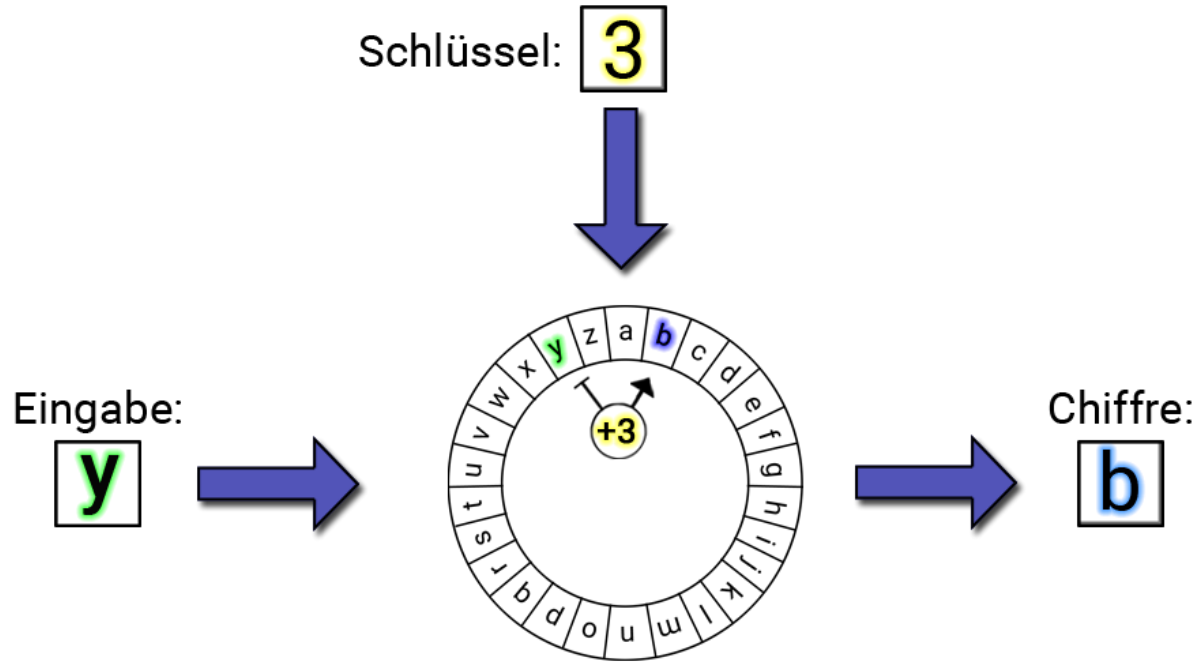
## Auftrag Nr. 4

Wende die Verschiebung um 6 Positionen auf die Nachricht „Julius“ an.

**Chiffre:** „ paroay “



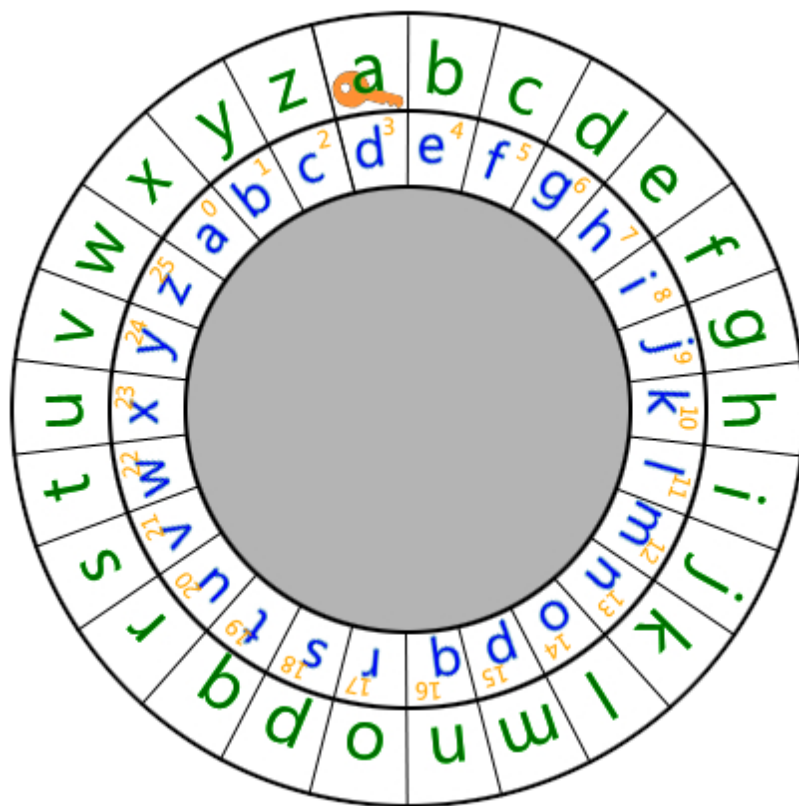
# Verschlüsseln mit Cäsar



## Die Cäsar-Scheibe



## Die Cäsar-Scheibe



## Verschlüsseln mit der Cäsar-Scheibe

- Stelle den **Schlüssel** auf der Cäsar-Scheibe ein.
- Außen: **Klartext**-Alphabet
- Innen: **Chiffre**-Alphabet
- Lese auf der Cäsar-Scheibe, für jeden **Klartext**-Buchstaben (**außen**) den **verschlüsselten** Buchstaben (**innen**) ab.

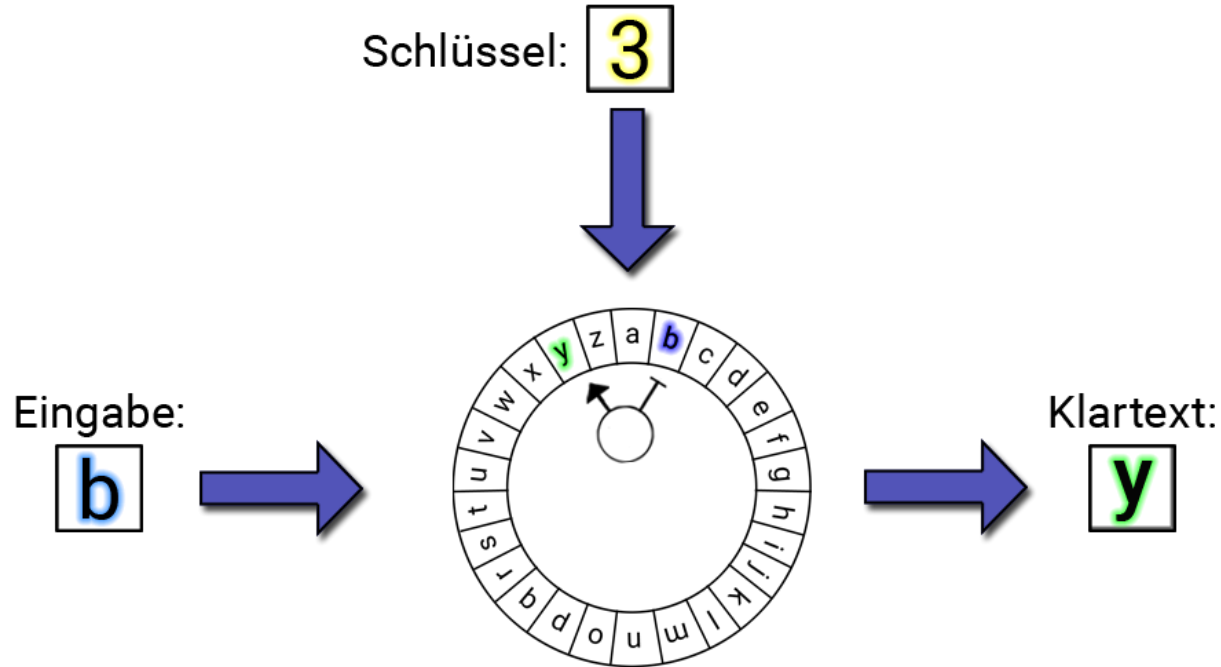


## Auftrag Nr. 5

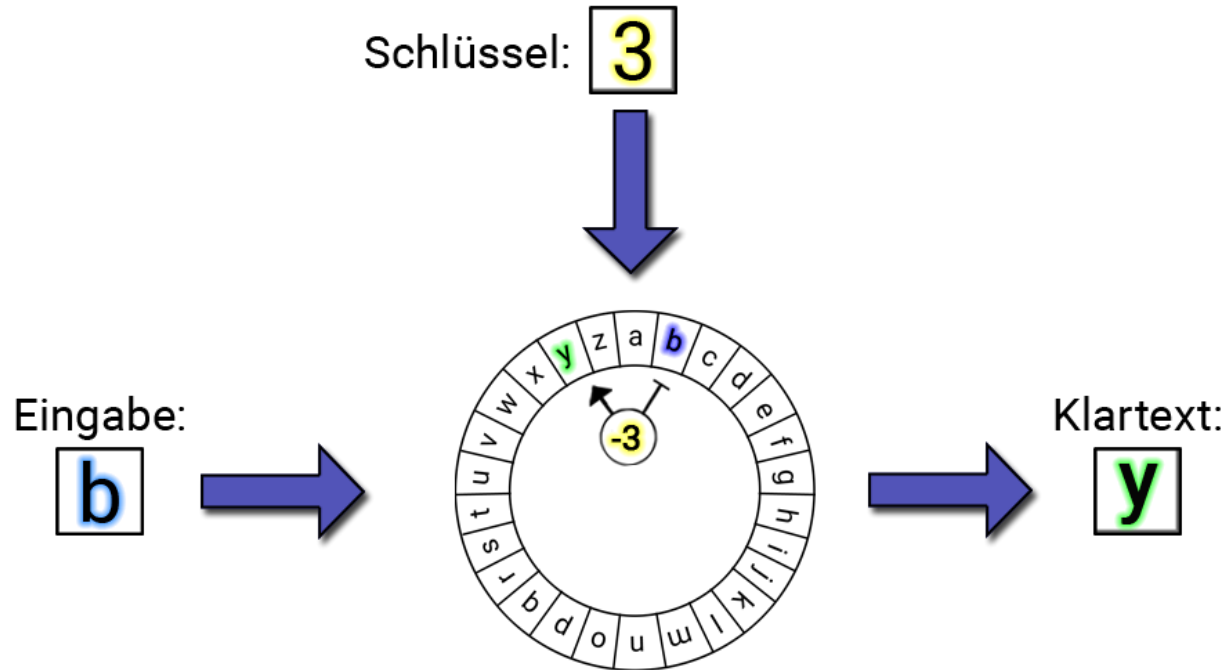


- Überlegt euch eine Nachricht und verschlüsselt diese mit einem beliebigen Schlüssel.
- Schreibt das Ergebnis auf einen Zettel und gebt diesen vorne ab.

# Entschlüsseln mit Cäsar



# Entschlüsseln mit Cäsar



## Entschlüsseln mit der Cäsar-Scheibe

- Stelle den **Schlüssel** auf der Cäsar-Scheibe ein.
- Außen: **Klartext**-Alphabet
- Innen: **Chiffre**-Alphabet
- Lese auf der Cäsar-Scheibe, für jeden **verschlüsselten** Buchstaben (**innen**) den zugehörigen **Klartext**-Buchstaben (**außen**) ab.





## Auftrag Nr. 6

- Entschlüssele die Chiffre: „motfgzs, sqrmtd!“.
- Der Schlüssel ist: „12“

(Zeichen, die im Chiffre-Alphabet nicht vorkommen werden einfach in den Klartext übernommen)

**Klartext:** „achtung, gefahr!“

## Sicherheit des Cäsar-Verfahrens



Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

- Alle Schlüssel ausprobieren

## Alle Schlüssel ausprobieren



- Entschlüssele die Chiffre mit jedem möglichen Schlüssel.
- Unter den Ergebnissen befindet sich der Klartext.



## Auftrag Nr. 7

- Knacke die Chiffre „cvyzpjoa“.
- Probiere so lange verschiedene Schlüssel aus, bis du einen sinnvollen Klartext erhältst.

**Schlüssel: 7**

**Klartext: „vorsicht“**

## Alle Schlüssel ausprobieren



- Entschlüssele die Chiffre mit jedem möglichen Schlüssel.
- Unter den Ergebnissen befindet sich der Klartext.
- Maximale Anzahl an Versuchen?

## Alle Schlüssel ausprobieren



- Entschlüssele die Chiffre mit jedem möglichen Schlüssel.
- Unter den Ergebnissen befindet sich der Klartext.
- Maximale Anzahl an Versuchen? 26 (25)

## Sicherheit des Cäsar-Verfahrens



Wie kann ein Angreifer aus einer Chiffre den Klartext erhalten, ohne den Schlüssel zu kennen?

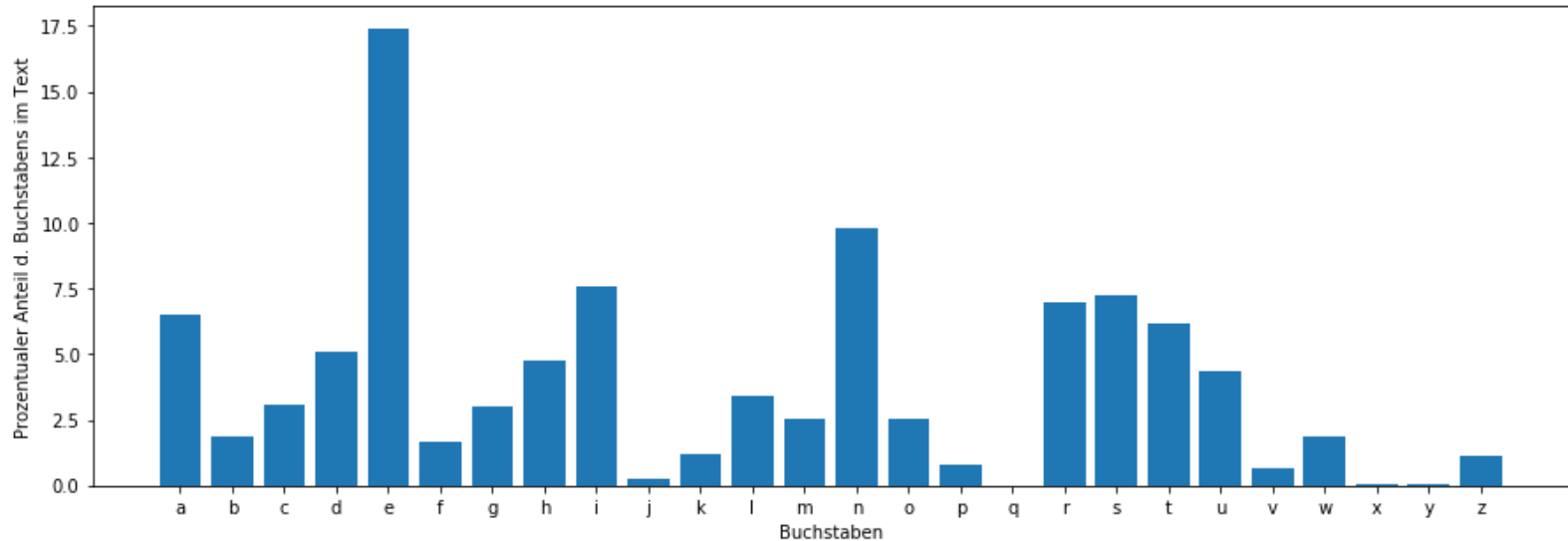
- Alle Schlüssel ausprobieren
- Häufigkeitsanalyse

## Häufigkeitsanalyse



- In jeder Sprache kommen bestimmte Buchstaben unterschiedlich häufig vor.

## Welcher Buchstabe kommt im Deutschen am häufigsten vor?



## Häufigkeitsanalyse



- In jeder Sprache kommen bestimmte Buchstaben unterschiedlich häufig vor.
- Im Deutschen: „e“
- Häufigste Buchstabe im Klartext: „e“
- Häufigste Buchstabe in der Chiffre?

## Auftrag Nr. 8



- Klartext: „Der Schatz liegt hinter dem Muelleimer“
- Welcher ist der häufigste Buchstabe im Klartext?
- Verschlüssel mit dem Schlüssel 7.
- Welcher ist der häufigste Buchstabe in der Chiffre?

**Chiffre:** „ghu vfkdw olhju klqwhu ghp pxhoo hlp hu“

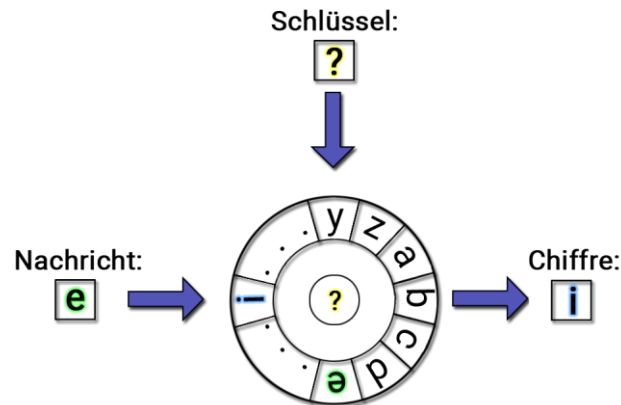


## Häufigkeitsanalyse

- In jeder Sprache kommen bestimmte Buchstaben unterschiedlich häufig vor.
- Im Deutschen: „e“
- Häufigste Buchstabe im Klartext: „e“
- Häufigste Buchstabe in der Chiffre?  
Der Buchstabe der herauskommt, wenn wir das „e“ verschlüsseln.

## Schlüssel bestimmen

- Häufigster Buchstabe in Chiffre: „i“
- Häufigster Buchstabe in Klartext:  
„e“ (wahrscheinlich)
- Schlüssel: 4



## Auftrag Nr. 9



- Chiffre: „qzvcgvijfe mvicrvjjk urj yrlj avuve dfixve  
vxve qvye lyi. yrckv dzty qlilvtb szj nvzkviv  
renvzjlexve vzekivwwve. ervtyjkvi bfekrbk  
lvsvidfifve.“
- Bestimme den verwendeten Schlüssel, indem du:
  - den häufigsten Buchstaben der Chiffre bestimmst,
  - die Cäsar-Scheibe so einstellst, dass der gefundene Buchstabe unter dem „e“ steht,
  - den Schlüssel beim „a“ abliest.

## Auftrag Nr. 9



- Chiffre: „qzvcgvijfe mvicrvjjk urj yrlj avuve dfixve  
xvxe qvye lyi. yrckv dzty qlilvtb szj nvzkviv  
renvzjlexve vzekivwwve. ervtyjkvi bfekrbk  
lvsvidfixve.“
- Bestimme den verwendeten Schlüssel, indem du:
  - den häufigsten Buchstaben der Chiffre bestimmst,
  - die Cäsar-Scheibe so einstellst, dass der gefundene Buchstabe unter dem „e“ steht,
  - den Schlüssel beim „a“ abliest.

Schlüssel: 17