

# Sicherheit des Cäsar-Verfahrens



## Sicherheit des Cäsar-Verfahrens

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



## Sicherheit des Cäsar-Verfahrens

- Wir wissen, beim Verschlüsseln wurde einer von 26 Schlüsseln verwendet und
- Benutzt man den richtigen Schlüssel, so macht die Entschlüsselung die Verschlüsselung rückgängig.



## Alle Schlüssel ausprobieren

Entschlüsselt man die Chiffre mit jedem möglichen Schlüssel, so befindet sich unter den Ergebnissen der Klartext.



## Verbesserung des Cäsar-Verfahrens

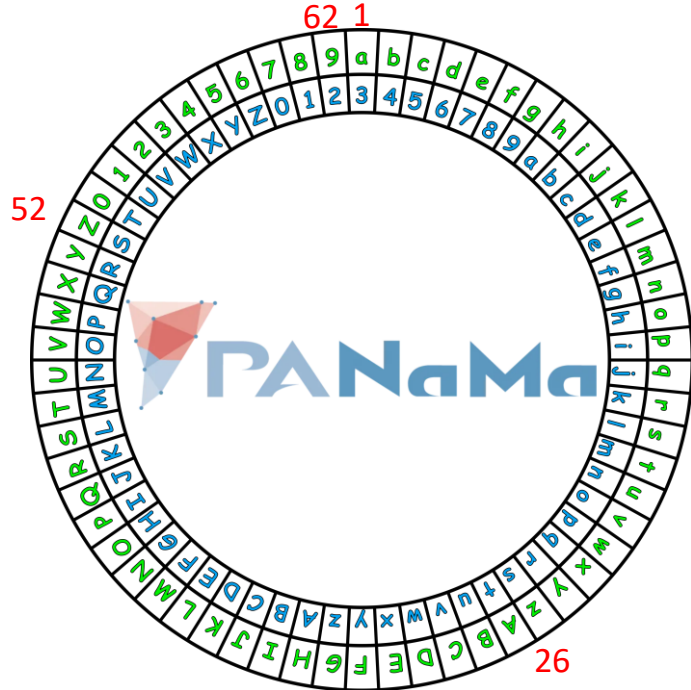
- **Problem:**

26 Schlüssel können sehr schnell ausprobiert werden

- **Lösung:**

Ändere das Verfahren so, dass mehr verschiedene Schlüssel verwendet werden können.

## Verbesserung des Cäsar-Verfahrens



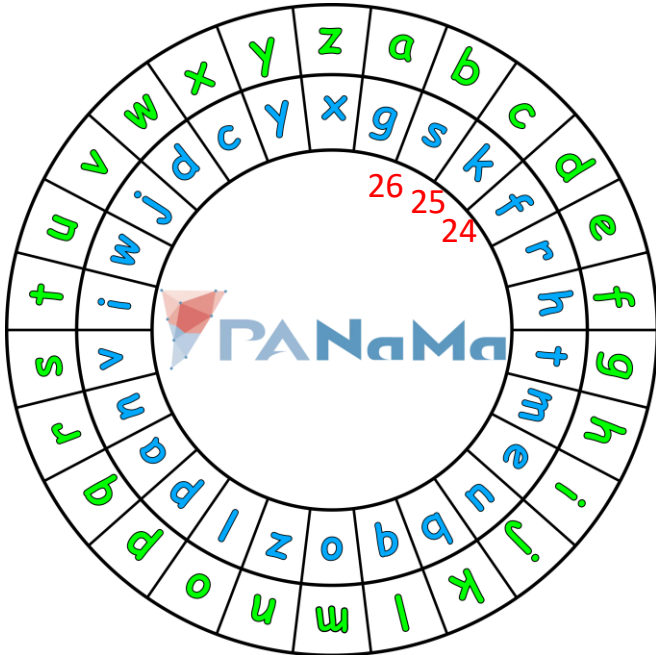
```

sonst wenn letter = "u" dann
  setze position auf 21
sonst wenn letter = "v" dann
  setze position auf 22
sonst wenn letter = "w" dann
  setze position auf 23
sonst wenn letter = "x" dann
  setze position auf 24
sonst wenn letter = "y" dann
  setze position auf 25
sonst wenn letter = "z" dann
  setze position auf 26
sonst wenn letter = "A" dann
  setze position auf 27
sonst wenn letter = "B" dann
  setze position auf 28
sonst wenn letter = "C" dann
  setze position auf 29
sonst wenn letter = "D" dann
  setze position auf 30
sonst wenn letter = "E" dann
  setze position auf 31
  
```

```

sonst wenn position = 21 dann
  setze letter auf "u"
sonst wenn position = 22 dann
  setze letter auf "v"
sonst wenn position = 23 dann
  setze letter auf "w"
sonst wenn position = 24 dann
  setze letter auf "x"
sonst wenn position = 25 dann
  setze letter auf "y"
sonst wenn position = 26 dann
  setze letter auf "z"
sonst wenn position = 27 dann
  setze letter auf "A"
sonst wenn position = 28 dann
  setze letter auf "B"
sonst wenn position = 29 dann
  setze letter auf "C"
sonst wenn position = 30 dann
  setze letter auf "D"
sonst wenn position = 31 dann
  setze letter auf "E"
  
```

## Verbesserung des Cäsar-Verfahrens



$$26 * 25 * 24 * 23 * \dots * 2 * 1 = 403.291.461.126.605.635.584.000.000$$

```

Funktion letterToPosition letter
wenn letter = "a" dann
  setze position auf 1
sonst wenn letter = "b" dann
  setze position auf 2
sonst wenn letter = "c" dann
  setze position auf 3
sonst wenn letter = "d" dann
  setze position auf 4
sonst wenn letter = "e" dann
  setze position auf 5
sonst wenn letter = "f" dann
  setze position auf 6
sonst wenn letter = "g" dann
  setze position auf 7
sonst wenn letter = "h" dann
  setze position auf 8
sonst wenn letter = "i" dann
  setze position auf 9
sonst wenn letter = "j" dann
  setze position auf 10
sonst wenn letter = "k" dann
  setze position auf 11

```

```

Funktion positionToLetter position
wenn position = 1 dann
  setze letter auf "a"
sonst wenn position = 2 dann
  setze letter auf "b"
sonst wenn position = 3 dann
  setze letter auf "c"
sonst wenn position = 4 dann
  setze letter auf "d"
sonst wenn position = 5 dann
  setze letter auf "e"
sonst wenn position = 6 dann
  setze letter auf "f"
sonst wenn position = 7 dann
  setze letter auf "g"
sonst wenn position = 8 dann
  setze letter auf "h"
sonst wenn position = 9 dann
  setze letter auf "i"
sonst wenn position = 10 dann
  setze letter auf "j"
sonst wenn position = 11 dann
  setze letter auf "k"

```

```

beim Start
  setze message auf "lets meet soon"
  setze chipher auf ""
  für Element letter von message
    mache
      setze position auf Aufruf letterToPosition letter
      setze new_letter auf Aufruf positionToLetter position
      setze chipher auf verbinde chipher new_letter
  seriell Zeile ausgeben chipher

```



## Anzahl möglicher Schlüssel

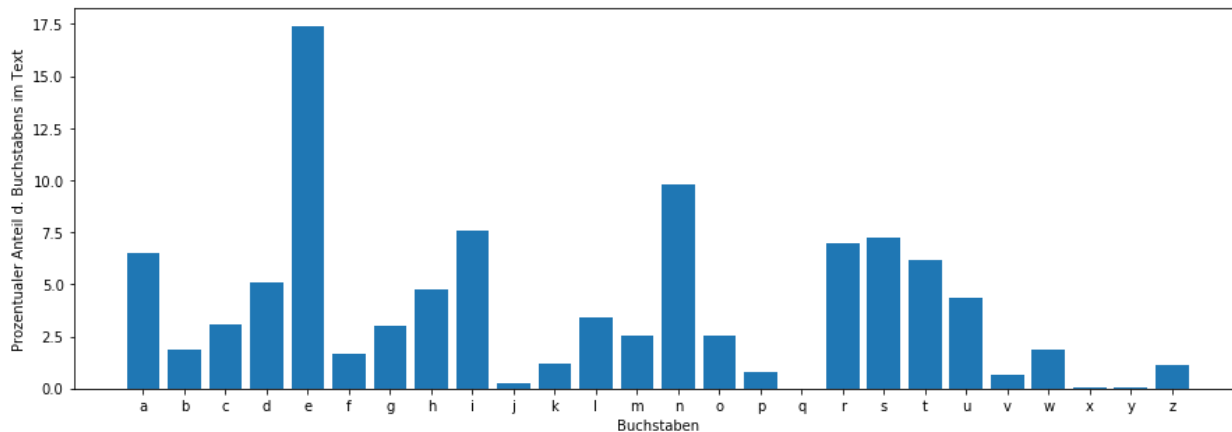
- Alphabet mit 26 Zeichen:  
403.291.461.126.605.635.584.000.000 (403 Quadrillion)
- Nicht sicher!



## Sicherheit des Cäsar-Verfahrens



In jeder Sprache kommen verschiedene Buchstaben unterschiedlich häufig vor.





## Häufigkeitsanalyse

- Im Deutschen kommt das *e* am häufigsten vor.
- Häufigste Buchstabe im Klartext: *e*
- Häufigste Buchstabe in der Chiffre?  
Der Buchstabe der herauskommt, wenn wir das *e* verschlüsseln.



## Häufigkeitsanalyse

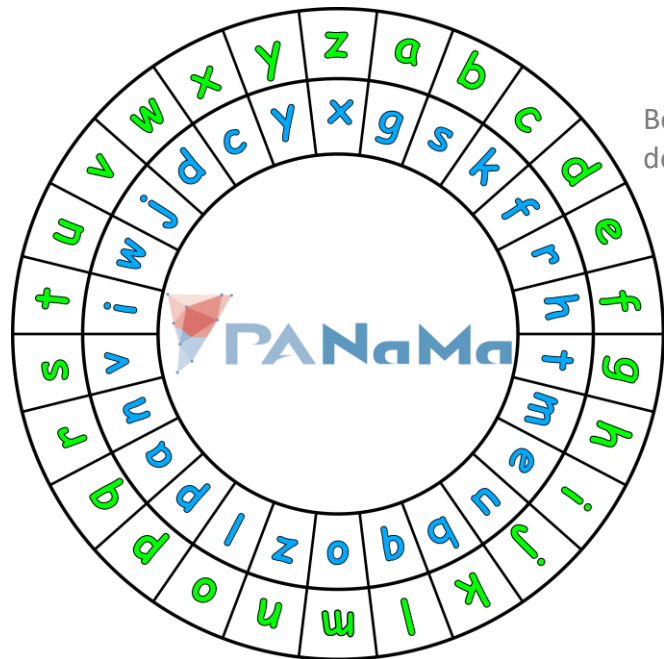
- Im Deutschen kommt das ***n*** am zweithäufigsten vor.
- Zweithäufigste Buchstabe im Klartext: ***n***
- Zweithäufigste Buchstabe in der Chiffre?  
Der Buchstabe der herauskommt, wenn wir das ***n*** verschlüsseln.
- Usw.



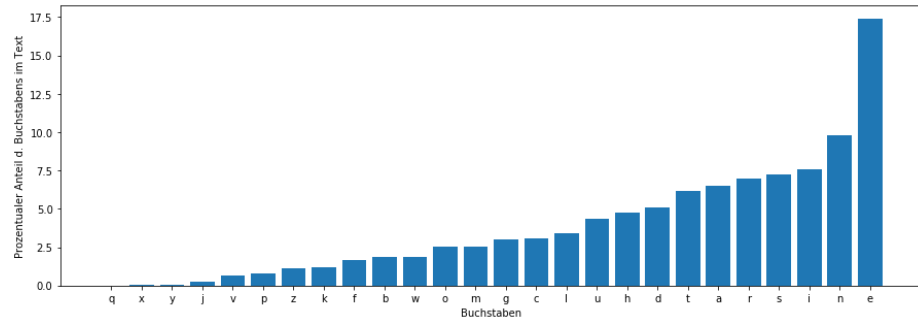
## Häufigkeitsanalyse

- Ist die verschlüsselte Nachricht lang genug, so können wir die Anzahl der verschiedenen Buchstaben zählen.
- Wie häufig ein Buchstabe in der Chiffre vorkommt gibt Aufschluss darüber, welchem Buchstaben er im Klartext entspricht.

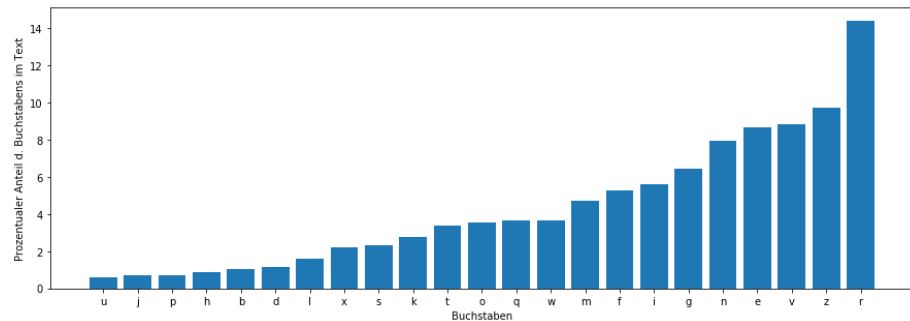
## Häufigkeitsanalyse



Beliebiger,  
deutscher Text:



Chiffre:





## Verbesserung des Cäsar-Verfahrens

- Problem:

Ein bestimmter Klartext-Buchstabe wird immer durch den gleichen Chiffre-Buchstaben ersetzt.

- Lösung:

Nicht nur der Buchstabe gibt vor wodurch er ersetzt wird, sondern auch, an welcher Position er im Text steht.

## Das Vigenère-Verfahren

- Namensgeber: Blaise de **Vigenère** (1523 –1596)
- Verbesserung der Cäsar-Verschlüsselung
- Mehr mögliche **Schlüssel**
- Schutz gegen **Häufigkeitsanalyse**
- Konnte erstmals um 1850 systematisch geknackt werden.



## Das Vigenère-Verfahren

- Buchstaben werden um verschiedene Werte verschoben
- Schlüssel besteht nicht aus einer Zahl, sondern aus mehreren, oder:
- (um sich den Schlüssel besser merken zu können) aus einem **Schlüsselwort**



## Beispiel



- Nachricht: „bewegung~~erwartet~~“
- Schlüssel: „hallo“

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

Schlüssel:

## Beispiel



- Nachricht: „bewegung~~erwartet~~“
- Schlüssel: „hallo“

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o |   |   |   |   |   |   |   |   |   |   |   |

Schlüssel:

## Beispiel



- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o |   |   |   |   |   |   |

Schlüssel:

## Beispiel



- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o | h | a | l | l | o |   |

Schlüssel:

## Beispiel



- Nachricht: „bewegungerwartet“
- Schlüssel: „hallo“

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o | h | a | l | l | o | h |

Schlüssel:

## Beispiel



Der Nachrichten-Buchstabe wird um den Schlüsselbuchstaben „verschoben“.

Nachricht:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o | h | a | l | l | o | h |

Schlüssel:

# Verschlüsseln mit der Vigenère-Tabelle



Nachricht:

Schlüssel:

Chiffre:

|   |   |   |   |   |
|---|---|---|---|---|
| b | e | w | e | g |
| h | a | l | l | o |
| i | e | h | p | u |

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

## Beispiel



Der Nachrichten-Buchstabe wird um den Schlüsselbuchstaben „verschoben“.

Nachricht:

Schlüssel:

Chiffre:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o | h | a | l | l | o | h |
| i | e | h | p | u | b | n | r | p | f | d | a | c | e | s | a |



## Beispiel

Der Nachrichten-Buchstabe wird um den Schlüsselbuchstaben „zurückgeschoben“.

**Nachricht:**

**Schlüssel:**

**Chiffre:**

|          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
|          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |          |
| <b>h</b> | <b>a</b> | <b>l</b> | <b>l</b> | <b>o</b> | <b>h</b> | <b>a</b> | <b>l</b> | <b>l</b> | <b>o</b> | <b>h</b> | <b>a</b> | <b>l</b> | <b>l</b> | <b>o</b> | <b>h</b> |
| <b>i</b> | <b>e</b> | <b>h</b> | <b>p</b> | <b>u</b> | <b>b</b> | <b>n</b> | <b>r</b> | <b>p</b> | <b>f</b> | <b>d</b> | <b>a</b> | <b>c</b> | <b>e</b> | <b>s</b> | <b>a</b> |

# Entschlüsseln mit der Vigenère-Tabelle

Nachricht:

|          |          |          |          |          |
|----------|----------|----------|----------|----------|
| <b>b</b> | <b>e</b> | <b>w</b> | <b>e</b> | <b>g</b> |
| <b>h</b> | <b>a</b> | <b>l</b> | <b>l</b> | <b>o</b> |
| <b>i</b> | <b>e</b> | <b>h</b> | <b>p</b> | <b>u</b> |

Schlüssel:

Chiffre:

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

## Beispiel

Der Nachrichten-Buchstabe wird um den Schlüsselbuchstaben „zurückgeschoben“.

Nachricht:

Schlüssel:

Chiffre:

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| b | e | w | e | g | u | n | g | e | r | w | a | r | t | e | t |
| h | a | l | l | o | h | a | l | l | o | h | a | l | l | o | h |
| i | e | h | p | u | b | n | r | p | f | d | a | c | e | s | a |

## Sicherheit des Vigenère-Verfahrens



- Der Schlüssel „**hallo**“ hat 5 Stellen.
- Alle möglichen 5-stelligen Schlüsselwörter:  

$$26 \cdot 26 \cdot 26 \cdot 26 \cdot 26 = 11.881.376$$
- Schlüssel mit 6 Stellen: 308.915.776
- Schlüssel mit 8 Stellen: 208.827.064.576
- Schlüssel mit 19 Stellen: besser als „Durcheinander“-Cäsar

## Zusammenfassung

- Das Cäsar-Verfahren ist sehr unsicher!
- Es gibt nur sehr wenige verschiedene Schlüssel & eine Häufigkeitsanalyse ist möglich.

## Zusammenfassung

- Mehr Schlüssel: „Durcheinander“-Cäsar
- Weniger anfällig gegen Häufigkeitsanalyse: Vigenère-Verfahren
- Das Vigenère-Verfahren ist unter bestimmten Umständen absolut sicher!