Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Cäsar mit dem PC

Wie sind wir beim Verschlüsseln vorgegangen?

- Einen Buchstaben wählen,
  - diesen verschieben,
  - zur Chiffre hinzufügen.
- Nächsten Buchstaben wählen,
  - diesen verschieben,
  - zur Chiffre hinzufügen.
- usw…

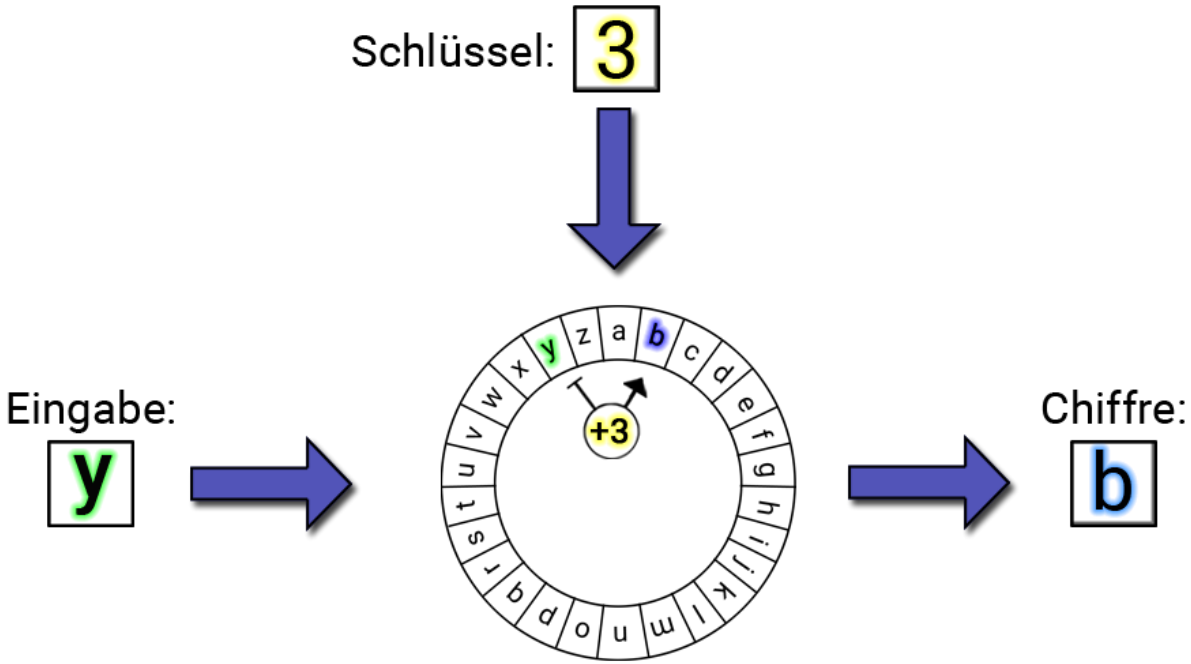
Problem beim Ver-/ und Entschlüsseln mit Cäsar

Aufwändig (langweilig) bei langen Nachrichten!

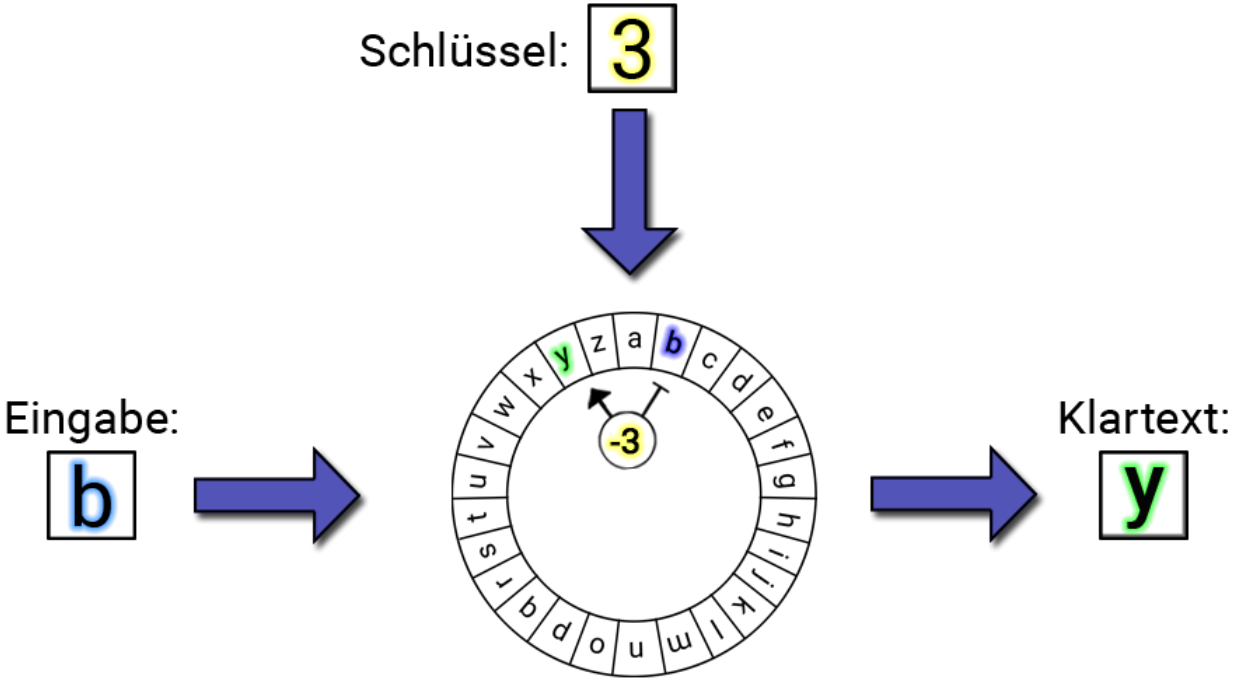
Lösung:

- Wir lassen den Computer die Arbeit machen.
- Der Computer versteht nur bestimmte, einfach Befehle.
- Deshalb müssen wir den Ver-/ und Entschlüsselungs-Prozess ein wenig anpassen.

Verschlüsseln mit Cäsar



Entschlüsseln mit Cäsar

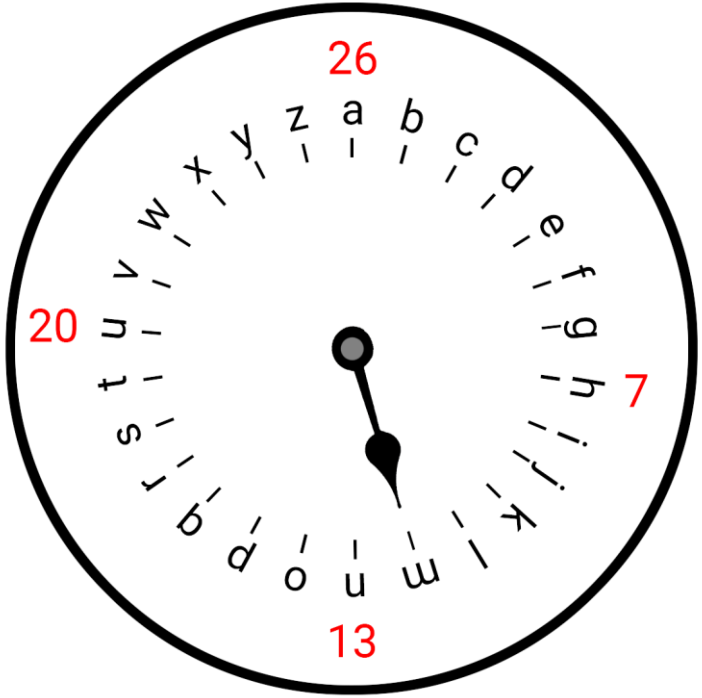


Buchstaben-Uhr

- Die Uhr hat 12 Stunden, wenn wir über 12 hinaus kommen, beginnen wir wieder bei der 1.

- Die Buchstaben-Uhr hat 26 Buchstaben, wenn wir über den 26. hinausschieben, beginnen wir wieder beim ersten.

Buchstaben-Uhr



Buchstaben-Uhr

- Wie bei der normalen Uhr beginnen wir bei 0 zu zählen (das „a“ ist bei „0 Uhr“).
- „a“ steht an Position 0
- „z“ steht an Position 25
- „m“ steht an Position 12

Buchstaben-Uhr

- Ist es 11 Uhr und es vergehen 3 Stunden, so ist es 2 Uhr.
- D.h. 11 + 3 „=“ 2 (**14** Uhr ist das gleiche wie **2** Uhr).

Buchstaben-Uhr

- Mathematisches Prinzip: **Division mit Rest**

  11 + 3 = 14

  14 : 12 = 1 Rest **2**

  14 = 1·12 + **2**

Beispiele

- **16** : 12 = 1 Rest **4**
- **23** : 12 = 1 Rest **11**
- **19** : 26 = 0 Rest **19**
- **45** : 26 = 1 Rest **19**

- **16** = 1·12 + **4**
- **23** = 1·12 + **11**
- **19** = 0·26 + **19**
- **45** = 1·26 + **19**

Auftrag Nr. 1

- **18** : 7 = …
- **28** : 15 = …
- **29** : 13 = …
- **42** : 17 = …

Auftrag Nr. 1

- **18** : 7 = 2 Rest **4**
- **28** : 15 = 1 Rest **13**
- **29** : 13 = 2 Rest **3**
- **42** : 17 = 2 Rest **8**

- **18** = 2· 7 + **4**
- **28** = 1·15 + **13**
- **29** = 2·13 + **3**
- **42** = 2·17 + **8**

Sprech-/ und Schreibweis

- Wir sagen: „18 modulo 7 ist gleich 4“
  („18 geteilt durch 7 hat den Rest 4“).
- Schreibweise: 18 (mod 7) = 4

  („18 modulo 7 ist gleich 4“)

- **28** : 15 = 1 Rest **13**
- **29** : 13 = 2 Rest **3**
- **42** : 17 = 2 Rest **8**

- **28** (mod 15) = **13**
- **29** (mod 13) = **3**
- **42** (mod 17) = **8**

Nutzen der Modulo-Rechnung

- Was der Computer nicht versteht:

  „Gebe den Buchstaben aus, der 3 weiter rechts steht.“

- Was der Computer versteht:

  „Jeder Buchstabe hat eine Zahl zugeordnet. Nehme die Zahl des Eingabe-Buchstaben und gebe den Buchstaben zurück, der diese (Zahl + 3) zugeordnet hat.“

Nutzen der Modulo-Rechnung

- Was der Computer nicht versteht:

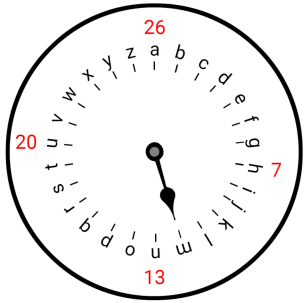
  „Schieben wir über das „z“ hinaus, beginnen wir wieder mit dem ‚a‘.“

- Was der Computer versteht:

  „Ist die Zahl größer als 26, nehme anstelle dieser den Rest der bei der Division durch 26 entsteht.“

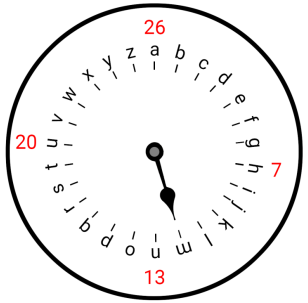
Cäsar am Computer

- „a“ wird mit Schlüsselwert 3 verschlüsselt
- Position von „a“: 0
- Position von „d“: 3
- 0 + 3 = 3



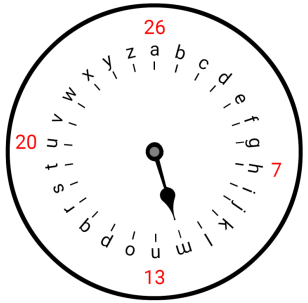
Cäsar am Computer

- „y“ wird mit Schlüsselwert 3 verschlüsselt
- Position von „y“: 24
- Position von „b“: 1
- 24 + 3 = 27
- 27 (mod 26) = 1



Cäsar am Computer

- „d“ wird mit Schlüsselwert 3 entschlüsselt
- Position von „d“: 3
- Position von „a“: 0
- 3 – 3 = 0



Cäsar am Computer

- „b“ wird mit Schlüsselwert 3 entschlüsselt
- Position von „b“: 1
- Position von „y“: 24
- 1 – 3 = - 2
- -2 (mod 26) = 24