

Cäsar mit MakeCode

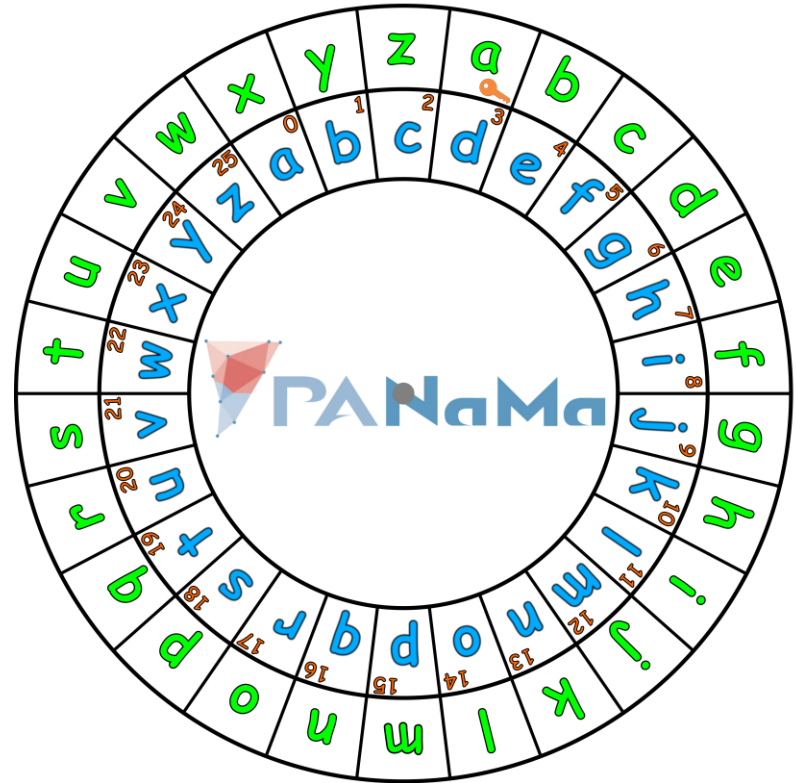
Problem beim Ver-/ und Entschlüsseln mit Cäsar

Problem:

- Der Computer versteht nur bestimmte, einfache Befehle.
- Deshalb müssen wir den Ver-/ und Entschlüsselungsprozess überdenken.

Was der Computer nicht versteht:

„Alle Buchstaben befinden sich auf einer Scheibe, außen die Klartextbuchstaben, innen die Chiffrebuchstaben und wenn du den Teil innen verdrehst stellst du einen anderen Schlüssel ein.“



Was kann der Computer?

- Zahlen & Text

- Einfache Operationen

- Zahlen: addieren, subtrahieren
- Text: verbinden

- Vergleichen

- Zahlen: $=$, $<$, $>$, \leq , \geq , \neq
- Text: $=$, \neq

Was kann der Computer?

- Die Operationen die uns beim Text zur Verfügung stehen helfen uns nicht beim „Verschieben“.
- Verschieben können wir nur Zahlen, durch addieren und subtrahieren.
- Übersetze Buchstaben in Zahlen

Übersetzung Buchstabe ↔ Zahl

Am einfachsten ist es wenn wir die Buchstaben abzählen.

Übersetzung Buchstabe ↔ Zahl

• a = 1

• h = 8

• o = 15

• v = 22

• b = 2

• i = 9

• p = 16

• w = 23

• c = 3

• j = 10

• q = 17

• x = 24

• d = 4

• k = 11

• r = 18

• y = 25

• e = 5

• l = 12

• s = 19

• z = 26

• f = 6

• m = 13

• t = 20

• g = 7

• n = 14

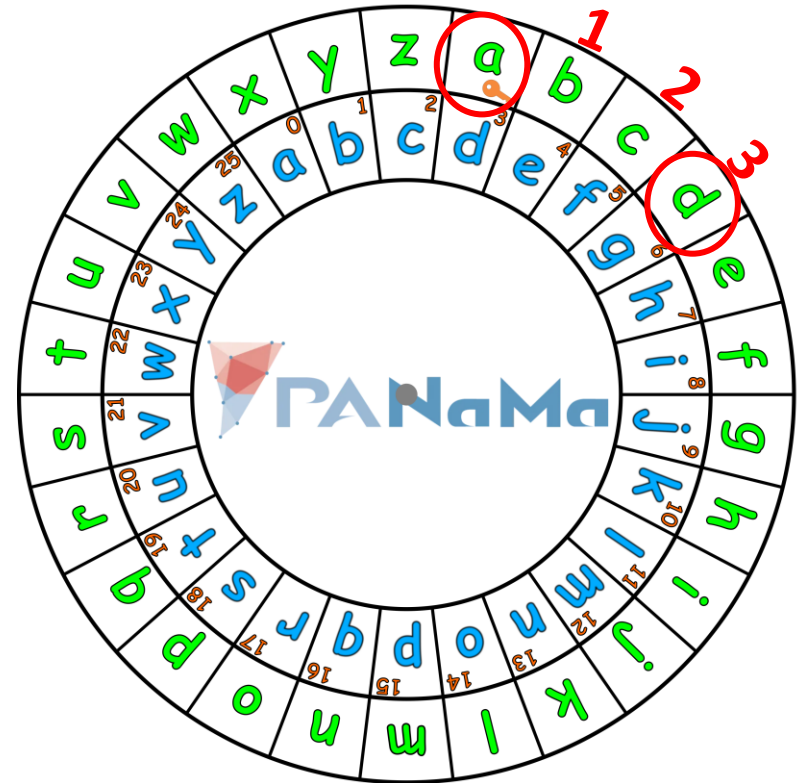
• u = 21

Übersetzung Buchstabe ↔ Zahl

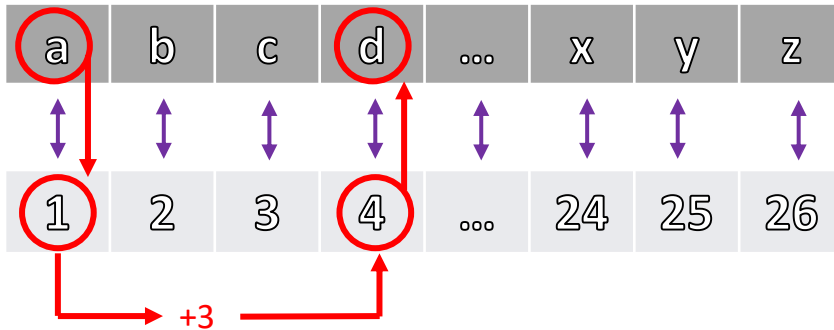
a	b	c	...	x	y	z
↕	↕	↕	↕	↕	↕	↕
1	2	3	...	24	25	26

Verschlüsseln mit dem Computer

a	b	c	d	...	x	y	z
↕	↕	↕	↕	↕	↕	↕	↕
1	2	3	4	...	24	25	26



Verschlüsseln mit dem Computer

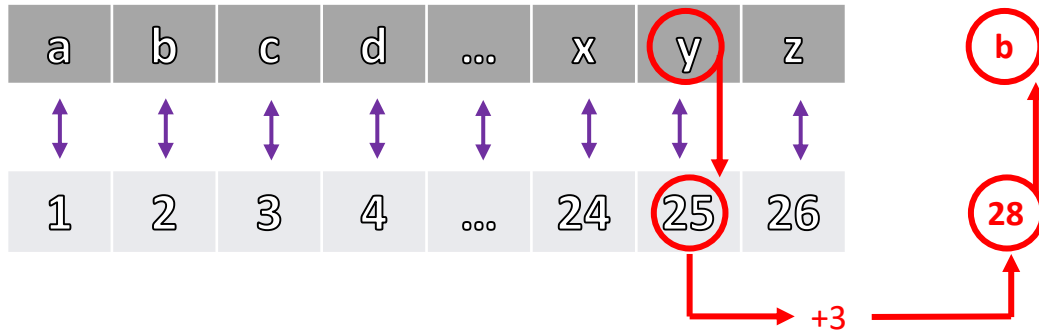


Schritt 1: Übersetze einen Buchstaben in eine Zahl

Schritt 2: Addiere den Schlüssel zur ermittelten Zahl

Schritt 3: Übersetze die neue Zahl wieder in einen Buchstaben

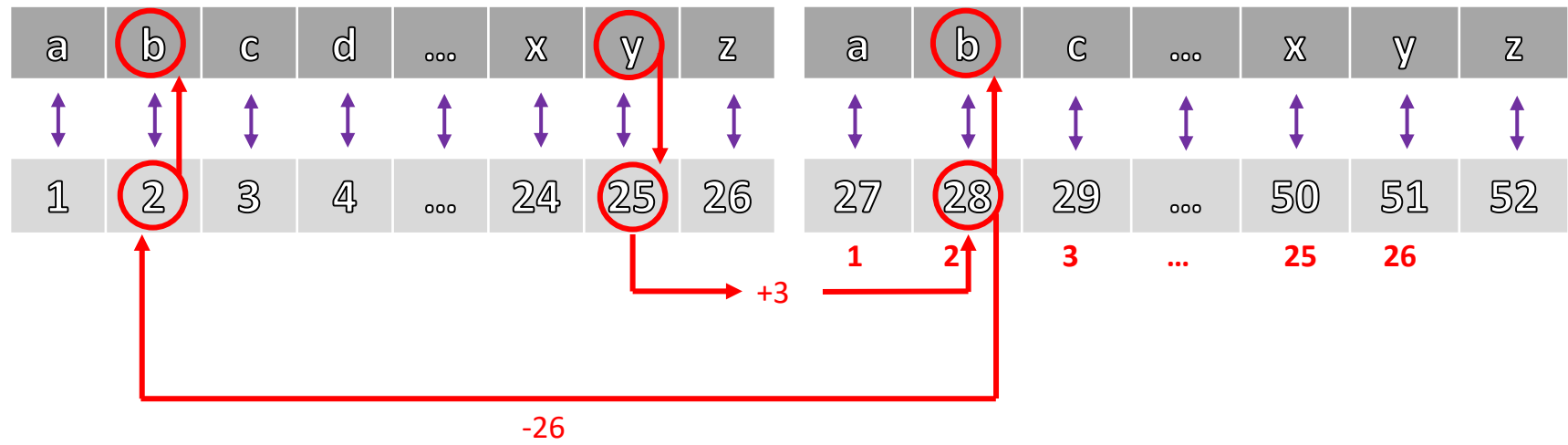
Verschlüsseln mit dem Computer



$$25 + 3 = 28$$

Verschlüsseln mit dem Computer

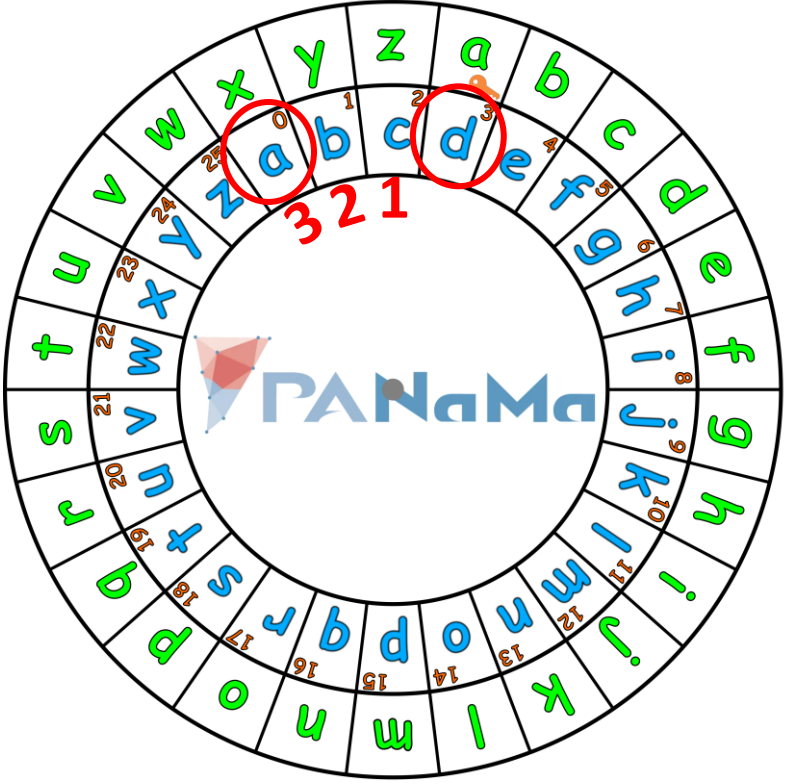
Wenn nach dem addieren des Schlüssels eine Zahl rauskommt, die größer als 26 ist, ziehe 26 ab.



Verschlüsseln mit dem Computer

- Schritt 1:
Übersetze einen Buchstaben in eine Zahl
- Schritt 2:
Addiere den Schlüssel zur ermittelten Zahl,
falls die Summe größer als 26 ist, ziehe 26 ab.
- Schritt 3:
Übersetze die neu Zahl wieder zurück in einen Buchstaben.

Entschlüsseln mit dem Computer



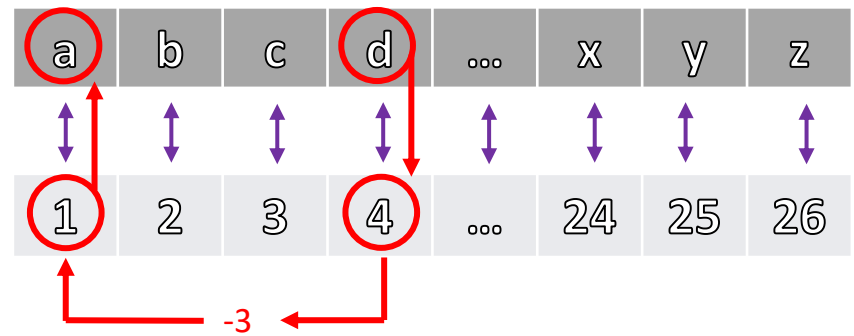
a	b	c	d	...	x	y	z
↕	↕	↕	↕	↕	↕	↕	↕
1	2	3	4	...	24	25	26

Entschlüsseln mit dem Computer

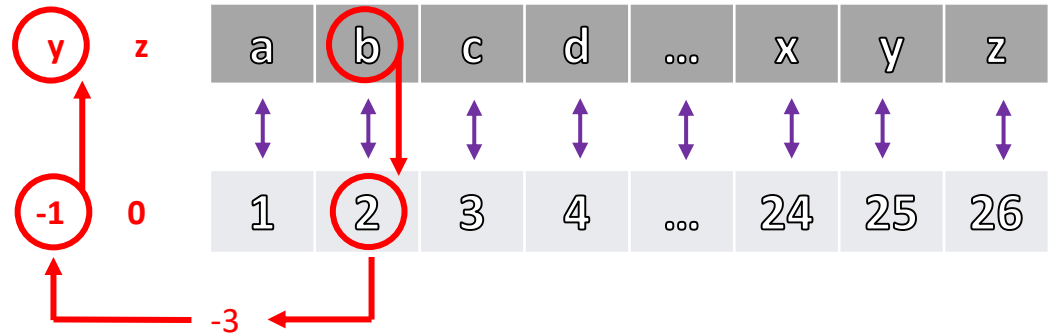
Schritt 1: Übersetze einen Buchstaben in eine Zahl

Schritt 2: Ziehe den Schlüssel von der ermittelten Zahl ab

Schritt 3: Übersetze die neu Zahl wieder in einen Buchstaben



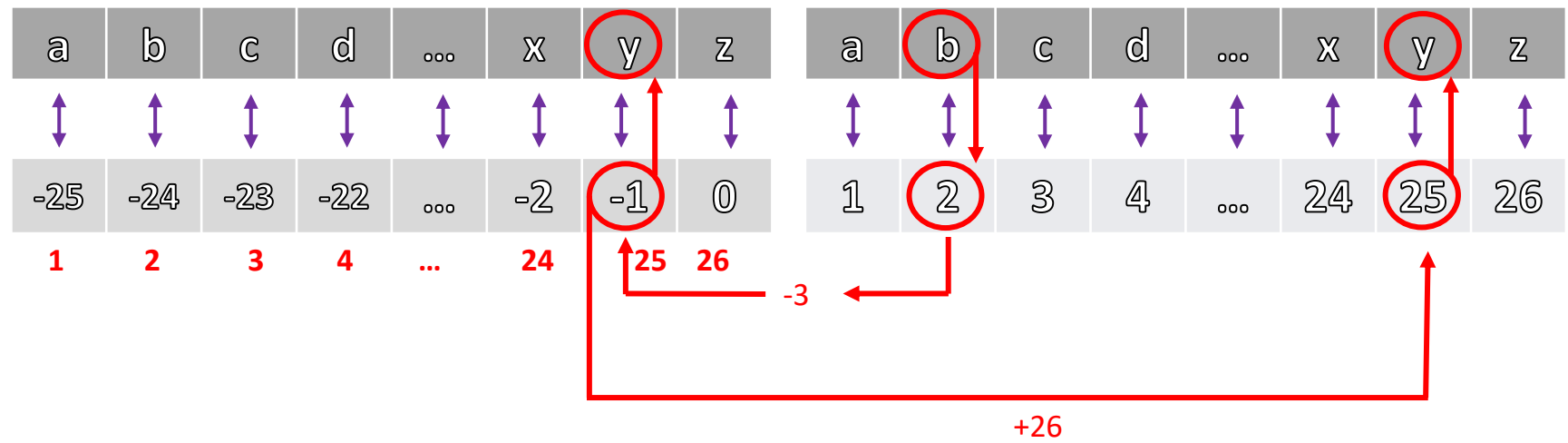
Entschlüsseln mit dem Computer



$$2 - 3 = -1$$

Entschlüsseln mit dem Computer

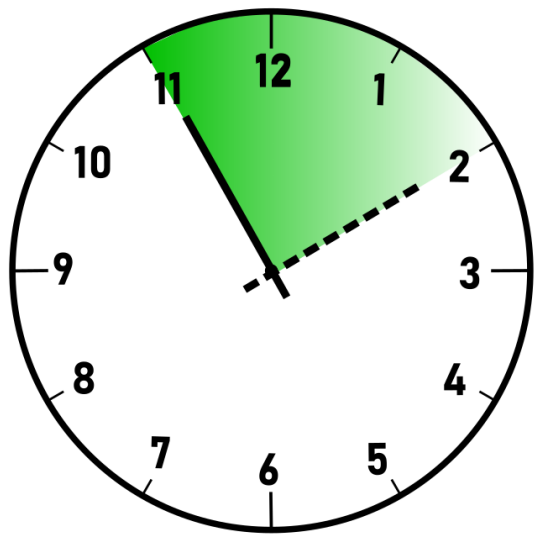
Wenn nach dem abziehen des Schlüssels eine Zahl rauskommt, die kleiner als 1 ist, addiere 26 hinzu.



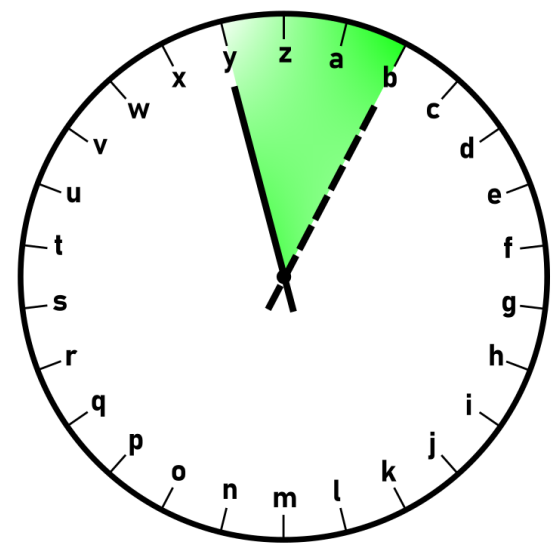
Verschlüsseln mit dem Computer

- Schritt 1:
Übersetze einen Buchstaben in eine Zahl
- Schritt 2:
Ziehe den Schlüssel von der ermittelten Zahl ab,
falls die Summe kleiner als 1 ist, addiere 26.
- Schritt 3:
Übersetze die neu Zahl wieder zurück in einen Buchstaben.

Das Prinzip ist bekannt!



+3h



+3

Das Prinzip ist bekannt!

- 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.

Zusammenfassung

- Damit der Computer die Arbeit übernehmen kann muss die Ver- und Entschlüsselung in einfachen Befehlen ausgedrückt werden.
- Buchstaben werden in Zahlen übersetzt und die „Verschiebung“ passiert durch addieren oder subtrahieren des Schlüsselwerts.
- Es muss sicherstellt werden, dass die Zahlen immer zwischen 1 und 26 liegen (nur denen sind Buchstaben zugeordnet)