Leibniz
Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der
Naturwissenschaften und Mathematik

The Caesar Cipher

www.ipn.uni-kiel.de

Where does the Caesar cipher origin from?

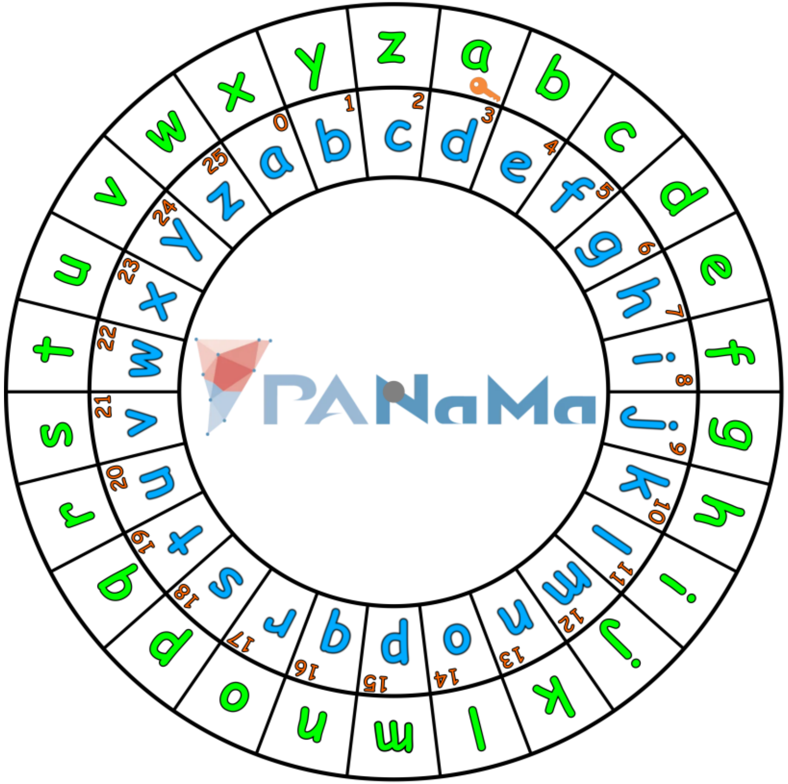
- Origin of name: Julius Gaius **Caesar**, 100-44 B.C.
- Encrypted communication for military purposes

How does it work?

- Each letter of the message is replaced by a specific other letter.
- The key determines by which one.

The Caesar disk

- The **plaintext** alphabet is on the outside of the disk,
- the **ciphertext** alphabet is on the inside.
- To **encrypt**, every plaintext letter is replaced by the ciphertext letter that is below it.


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 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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
PANaMa

Premise for the whole workshop:

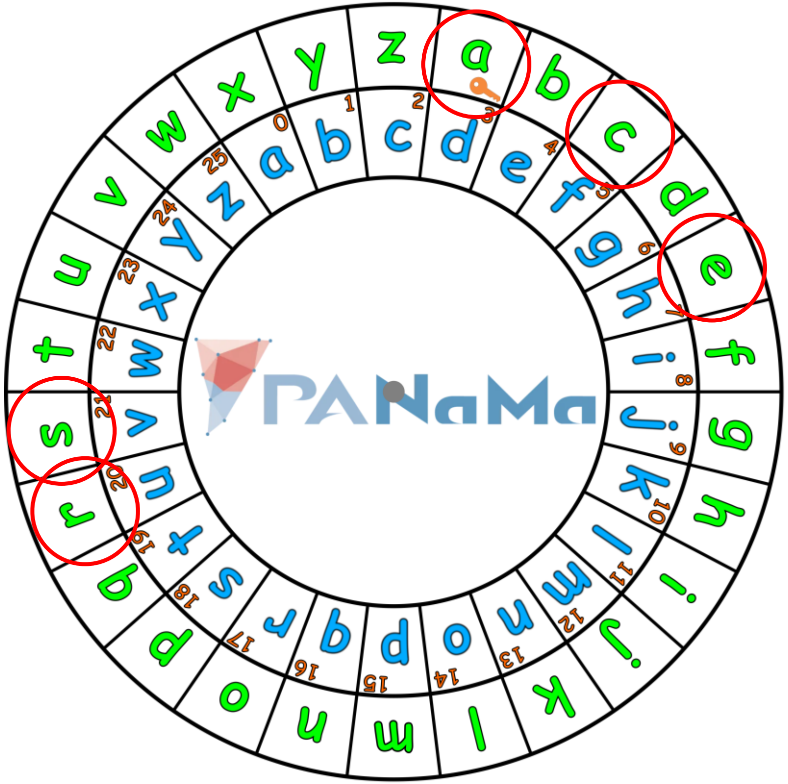
Only lower case letters from the latin alphabet are allowed (a-z)

Example

- **Message**: „Caesar“
- Adjusted to the alphabet that we want to use: „**caesar**“

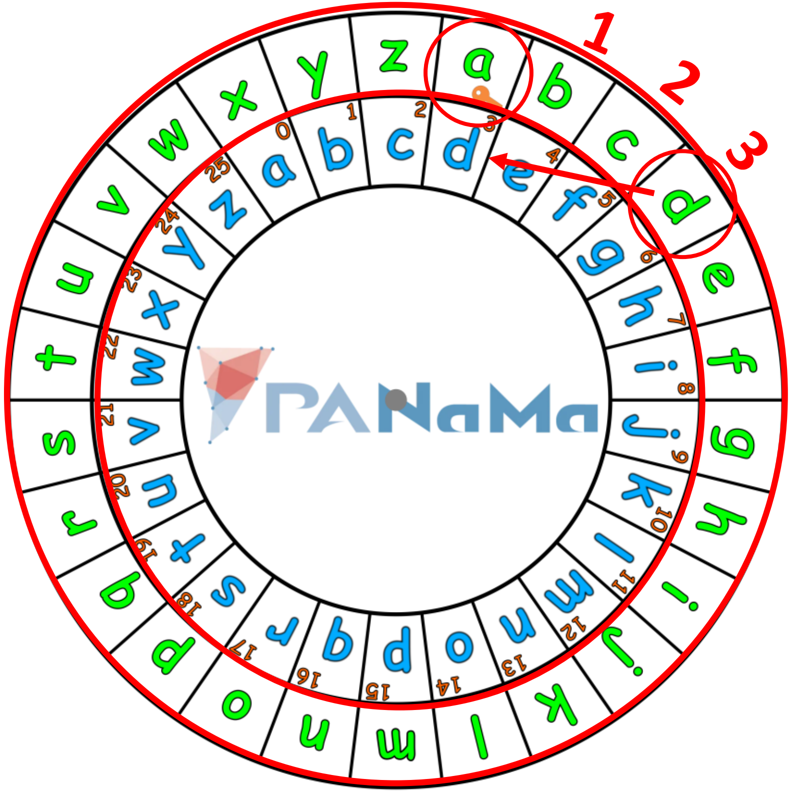
c	a	e	s	a	r
f	**d**	**h**	**v**	**d**	**u**

- **Ciphertext**: „fdhvdu“


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 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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
PANaMa

Which key was used?

- Every letter of the plaintext is replaced by the letter that is 3 positions further (clockwise).

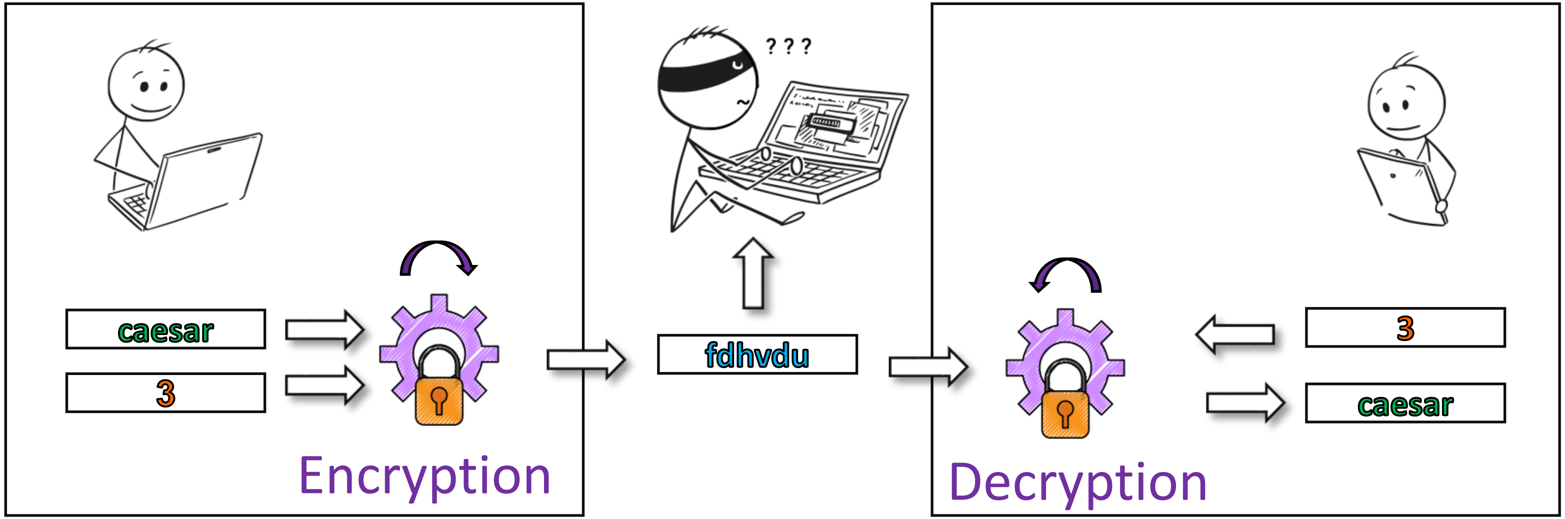


Which key was used?

Caesar used the key value **3**, but we can also use every (whole) number!

- To adjust the Caesar disk for different **key** values, you can rotate the inner disk.

Example



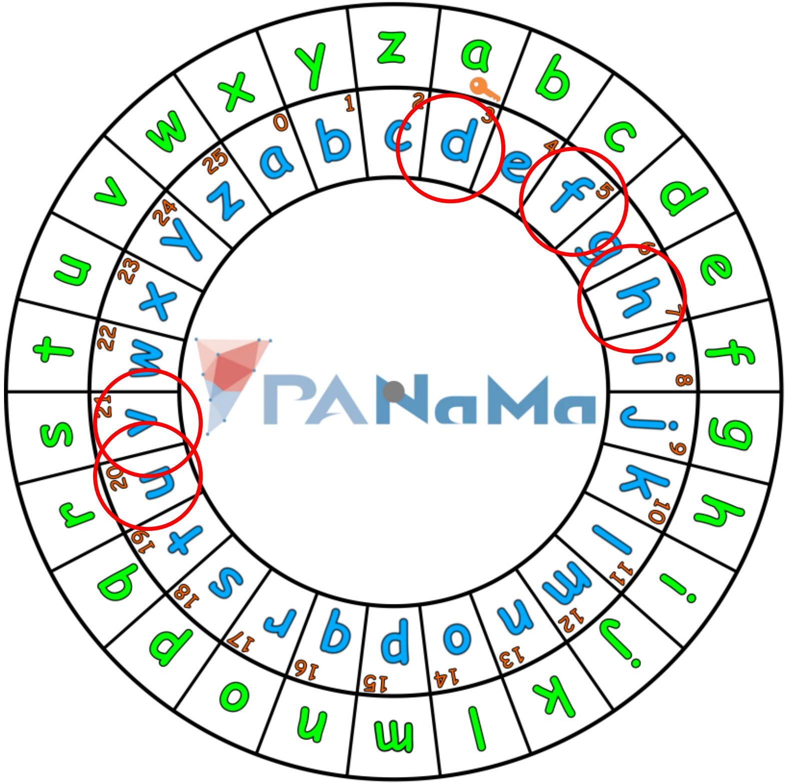
The sender and the recipient agreed on the key value 3. The attacker doesn‘t know this value.

How to undo the encryption

- To **decrypt** a message, each ciphertext letter is replaced by the letter above it.
- **Ciphertext**: „ fdhvdu“

c	a	e	s	a	r
f	d	h	v	d	u

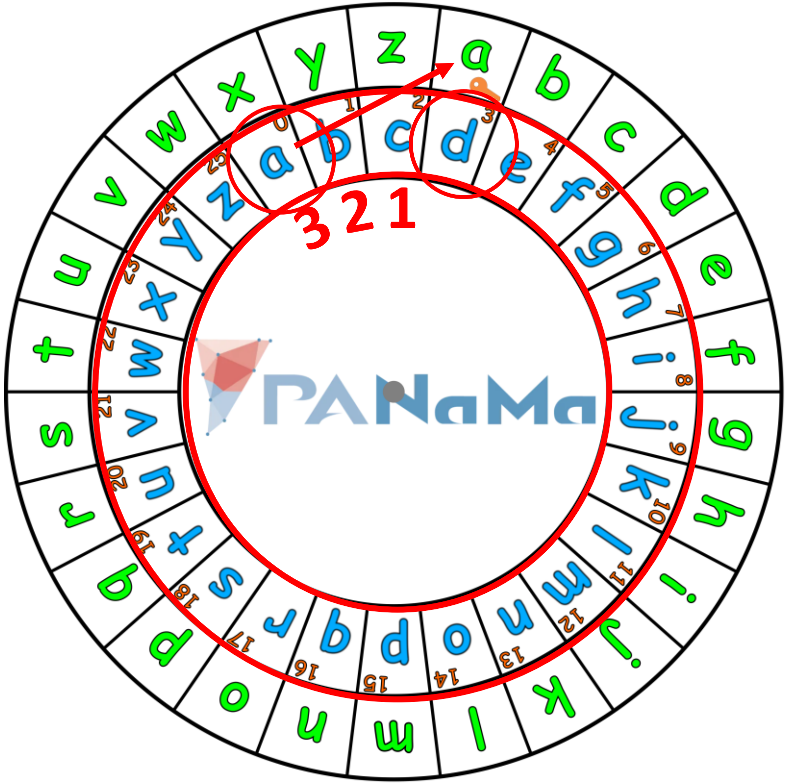
- **Plaintext**: „caesar“



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
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
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
PANaMa

Which key is used?

- Every letter of the ciphertext is replaced by the letter that is 3 positions further back (counter clockwise).



Summary

- The Caesar cipher encrypts and decrypts by replacing letters.
- With the Caesar disk: replace the letter outside by the letter inside (**encrypt**) or the letter inside by the letter outside (**decrypt**).
- **Key**: The number of positions we shift by.