Leibniz Gemeinschaft

IPN
Leibniz-Institut für die Pädagogik der Naturwissenschaften und Mathematik

Das Cäsar-Verfahren

Woher kommt das Cäsar-Verfahren?

- Namensgeber: Julius Gaius **Cäsar**, 100-44 v. Chr.

- Verschlüsselte Kommunikation für militärische Zwecke

Die Cäsar-Verschlüsselung

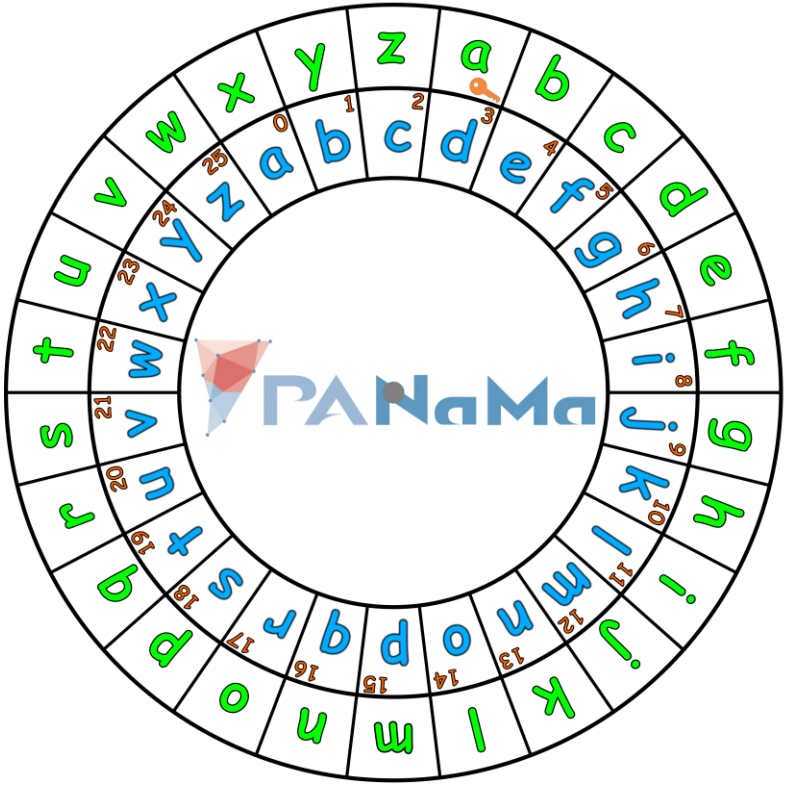
Wie funktioniert es?

- Jeder einzelne Buchstabe der Nachricht wird durch einen bestimmten Anderen ersetzt.

- Der **Schlüssel** bestimmt durch welchen

Die Cäsar-Scheibe

- Außen auf der Scheibe befindet sich das **Klartext**-Alphabet,
- innen das **Chiffre**-Alphabet.
- Beim **Verschlüsseln** wird jeder Klartextbuchstabe durch den unter ihm stehenden Chiffrebuchstaben ersetzt.



Voraussetzung für den (ganzen) Workshop:

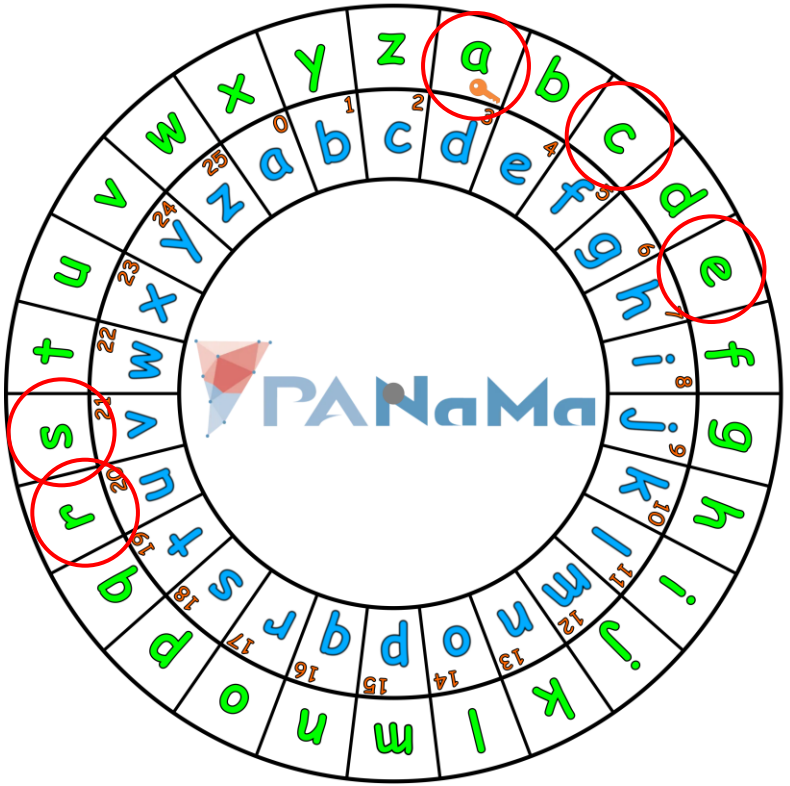
Nur Kleinbuchstaben aus dem lateinischen Alphabet (a-z) sind erlaubt.

Beispiel

- **Nachricht**: „Cäsar“
- Angepasst an das Alphabet, das wir benutzen wollen: „**caesar**“

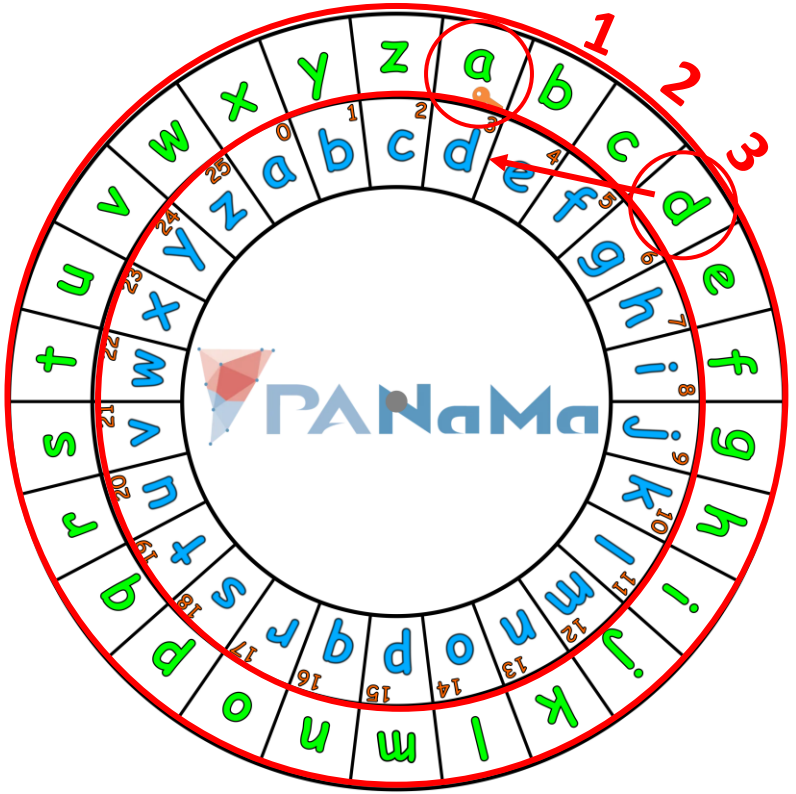
c	a	e	s	a	r
f	d	h	v	d	u

- **Chiffre**: „**fdhvdu**“



Welcher Schlüssel wurde verwendet?

- Jeder Buchstabe des Klartexts wird durch den Buchstaben ersetzt, der **3** Stellen weiter (im Uhrzeigersinn) steht.

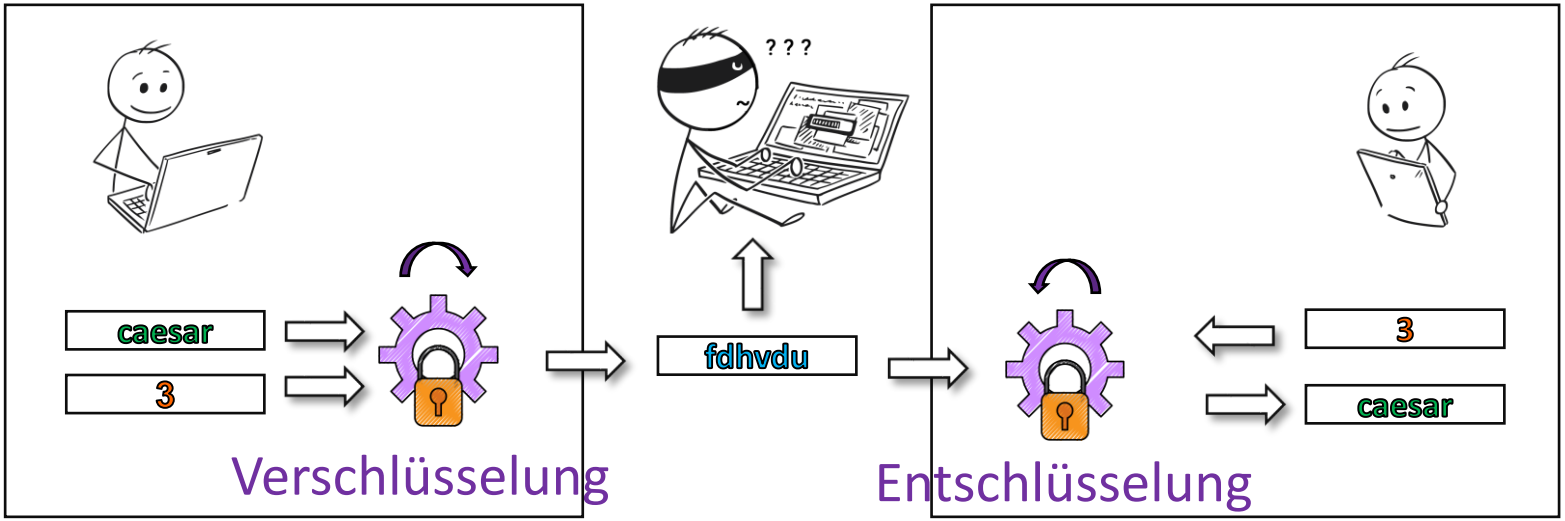


Welcher Schlüssel wurde verwendet?

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

- Damit man auf der Cäsar-Scheibe verschiedene **Schlüssel**-Werte einstellen kann, ist der innere Teil verdrehbar.

Beispiel



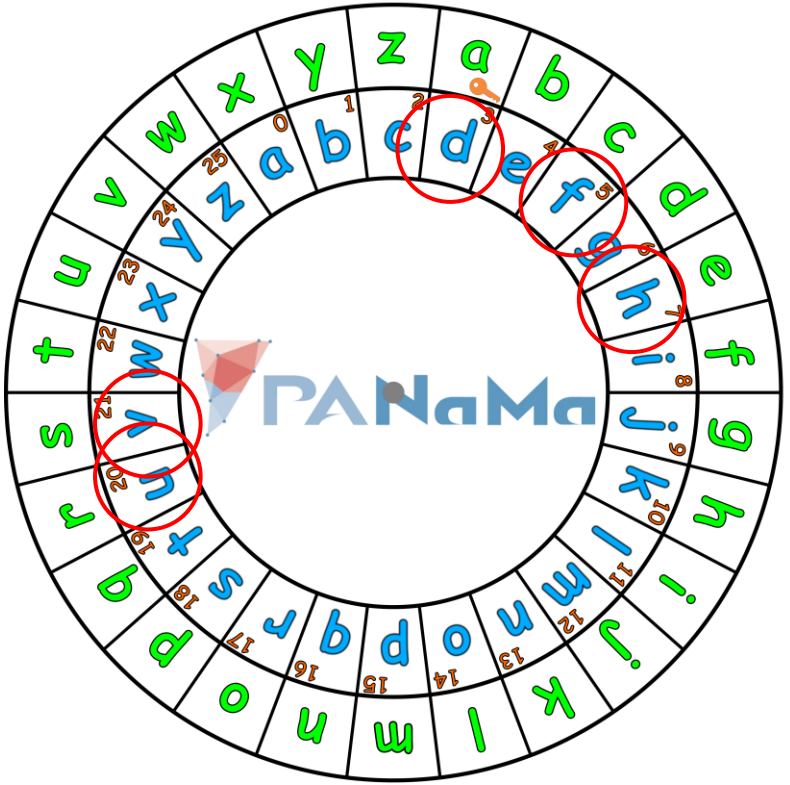
Der Sender und der Empfänger haben den Schlüsselwert **3** abgemacht, diesen kennt der Angreifer nicht.

Wie wird die Verschlüsselung rückgängig gemacht?

- Beim **Entschlüsseln** wird jeder Chiffrebuchstabe durch den über ihm stehenden Klartextbuchstabe ersetzt.
- **Geheimtext**: „ **fdhvdu**“

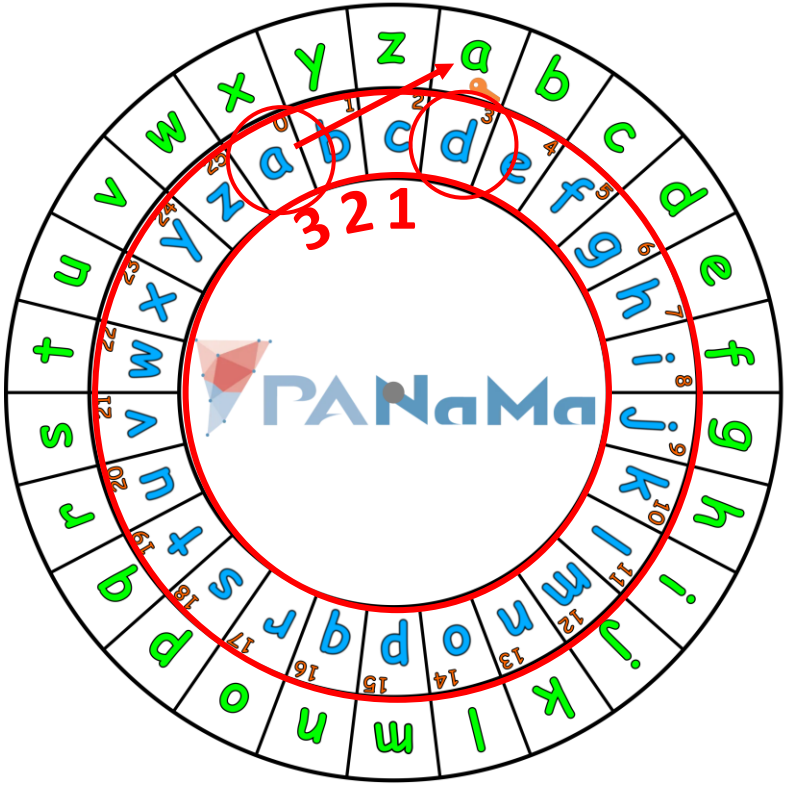
c	a	e	s	a	r
f	d	h	v	d	u

- **Klartext**: „**caesar**“



Welcher Schlüssel wurde verwendet?

- Jeder Buchstabe der Chiffre wird durch den Buchstaben ersetzt, der **3** Stellen vor ihm steht (gegen den Uhrzeigersinn).



Zusammenfassung

- Bei dem Cäsar-Verfahren wird ver- und entschlüsselt, indem Buchstaben **ausgetauscht** werden.

- Mit der Cäsar-Scheibe: Den Buchstaben außen durch den innen (**verschlüsseln**) oder den Buchstaben innen durch den außen (**entschlüsseln**) ersetzen.

- **Schlüssel**: Die Stellen um die ein Buchstabe verschoben wird.