

## Agenda zu Verschlüsselung

- Kryptographie
- Verschlüsselung
- Monoalphabetische Verschlüsselung
- Cäsar-Verschlüsselung

# Kryptographie

## Grundlagen

## Was bedeutet Kryptographie?

Die **Wissenschaft**, die sich mit dem **Schutz von Informationen** (z.B. bei der Kommunikation) beschäftigt. Dazu nutzt sie Methoden wie die **Verschlüsselung**.



Ohne Kryptographie gibt es keine echte Privatsphäre im Internet!

# Verschlüsselung

## Grundlagen

## Was ist Verschlüsselung und welches Ziel hat sie?

Umwandlung von "**Klartext**" in "**Geheimtext**". Dies geschieht mit Hilfe eines **geheimen Schlüssels**.

**Ziel:** Daten für Unbefugte unverständlich machen!



## Der Unterschied zw. Verschlüsselung und Kodierung

 **Verschlüsselung:**

**Informationen für Unbefugte unverständlich machen.**

 **Kodierung:**

**Informationen für Maschinen oder Menschen verständlicher machen (z.B. Binärcode oder Braille).**

---

## Warum brauchen wir Verschlüsselung?

Verschlüsselung schützt Daten auf unsicheren Übertragungswegen wie Internet oder WLAN.

Es ermöglicht Vertraulichkeit und Integrität.

- **Vertraulichkeit:** Informationen bleiben vor Unbefugten verborgen.
- **Integrität:** Informationen können nicht unbemerkt verändert werden.

# Monoalphabetisch Verschlüsselung

## Monoalphabetische Verschlüsselung

Der Name kommt von "**mono**" (einzeln) und "**Alphabet**" ab.

- Prinzip: **Jedes Zeichen** vom **Klartext** wird immer durch **dasselbe Zeichen** aus dem **Geheimtextalphabet** ersetzt.
  - ▶ Man nennt das „**Einfache Substitution**“ (= Einfache Ersetzung).

Solche Verfahren gelten als unsicher, weil sie heute leicht gebrochen werden können (Durch „Häufigkeitsanalyse“).

---

# Cäsar-Verschlüsselung

## Buchstaben verschieben

## Cäsar-Verschlüsselung

|                    |   |   |   |   |   |
|--------------------|---|---|---|---|---|
| <b>Klartext:</b>   | H | A | L | L | O |
| <b>Schlüssel:</b>  | 1 |   |   |   |   |
| <b>Geheimtext:</b> | I | B | M | M | P |

Schlüssel  
ist Zahl

Jeder **Buchstabe** vom Klartext wird um eine bestimmte Anzahl von Stellen im Alphabet **verschoben**, wodurch Geheimtext entsteht.

### Fazit:

Sehr **unsicher** und nur zu **Lernzwecken** verwendet!

## Normale Cäsar-Verschlüsselung



## Umgekehrte Cäsar-Verschlüsselung



## Übung

Verschlüsseln Sie folgende Texte mittels Cäsar-Verschlüsselung.

**Klartext      Schlüssel      Geheimtext**

|       |   |       |
|-------|---|-------|
| HALLO | 1 | IBMMP |
| HALLO | 2 | JCNNQ |
| WELT  | 3 | ZHOW  |
| WELT  | 1 | XFMU  |

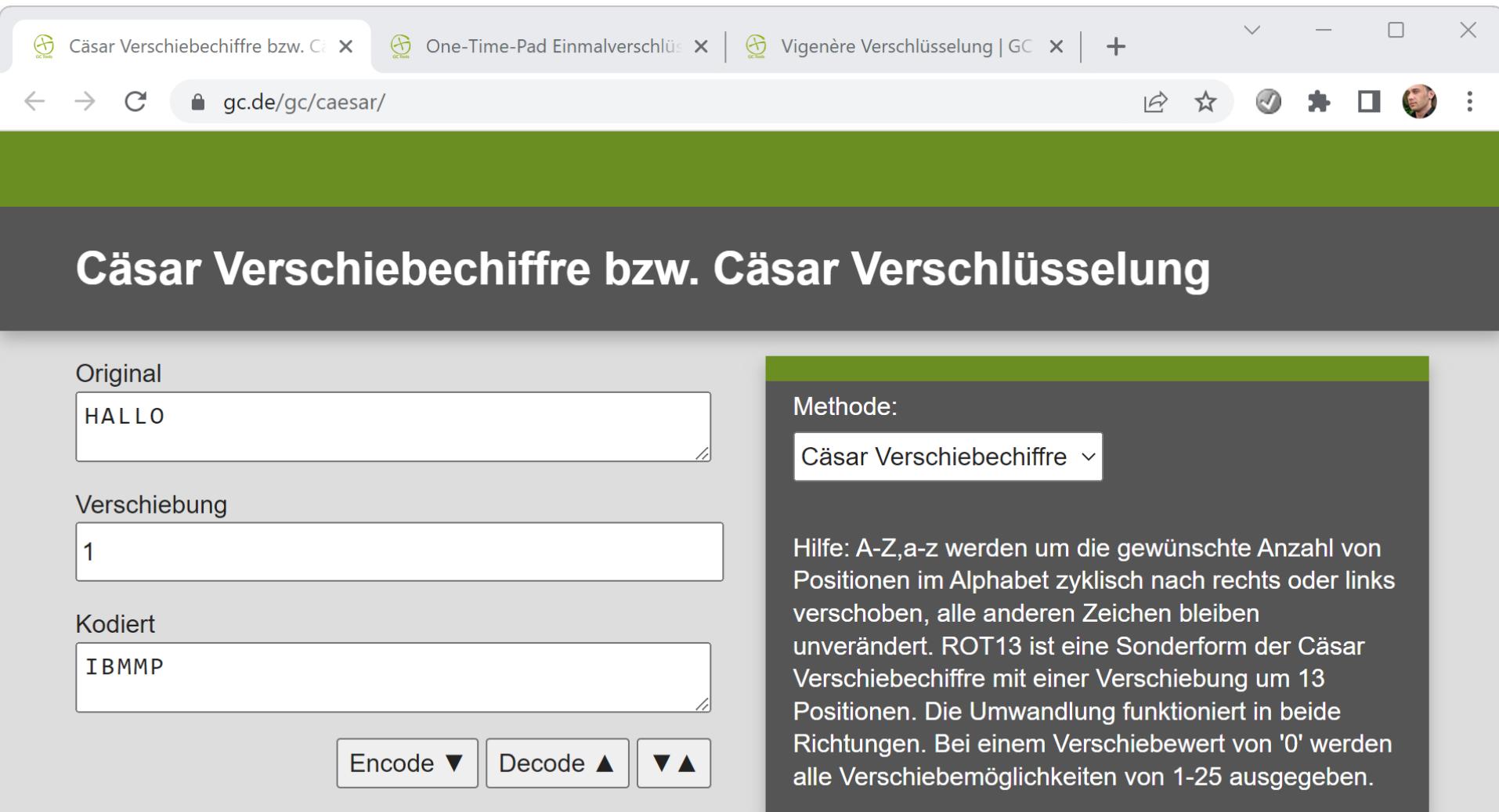
## Übung

Entschlüsseln Sie folgende Texte mittels Cäsar-Verschlüsselung.

**Geheimtext    Schlüssel    Klartext**

|       |   |       |
|-------|---|-------|
| UFYU  | 1 | TEXT  |
| OCWU  | 2 | MAUS  |
| FRGH  | 3 | CODE  |
| EBUFO | 1 | DATEN |

## Webseite: <https://gc.de/gc/caesar>



The screenshot shows a web browser window with three tabs open:

- Cäsar Verschiebechiffre bzw. Cäsar Verschlüsselung (active tab)
- One-Time-Pad Einmalverschlüsselung
- Vigenère Verschlüsselung | GC

The main content area displays the Caesar Cipher tool:

**Cäsar Verschiebechiffre bzw. Cäsar Verschlüsselung**

Original: HALLO

Verschiebung: 1

Kodiert: IBMMP

Buttons: Encode ▼, Decode ▲, ▼▲

Methode: Cäsar Verschiebechiffre

Hilfe: A-Z,a-z werden um die gewünschte Anzahl von Positionen im Alphabet zyklisch nach rechts oder links verschoben, alle anderen Zeichen bleiben unverändert. ROT13 ist eine Sonderform der Cäsar Verschiebechiffre mit einer Verschiebung um 13 Positionen. Die Umwandlung funktioniert in beide Richtungen. Bei einem Verschiebewert von '0' werden alle Verschiebemöglichkeiten von 1-25 ausgegeben.