# Datenschutz & Datensicherheit

# Quiz

- Darf Facebook deine Fotos verkaufen?
- „Du gewährst uns eine übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jedweder Inhalte, die du auf bzw. im Zusammenhang mit Facebook postest.“

Quelle: https://www.facebook.com/terms (abgerufen am 27.01.2017)

Das heißt: kostenlose Nutzung, Verkauf (Unterlizenz) für alle deine Inhalte durch Facebook

# Quiz

- Darf WhatsApp deine Selfies nutzen?
- Damit wir unsere Dienste betreiben [... ] gewährst du WhatsApp eine weltweite, gebührenfreie, unterlizenzierbare und übertragbare Lizenz zur Nutzung,  Verbreitung, Erstellung abgeleiteter Werke, Darstellung und Aufführung der Informationen (einschließlich der Inhalte), die du auf bzw. über unsere/n Dienste/n [...] sendest oder empfängst.

Quelle: https://www.whatsapp.com/legal/?l=de#terms-of-service (abgerufen am 27.01.2017)

Das heißt: Deine Fotos und Texte können von WhatsApp kostenlos genutzt und auch verändert werden (abgeleitete Werke), bevor sie verkauft (Unterlizenz) werden.

# Quiz

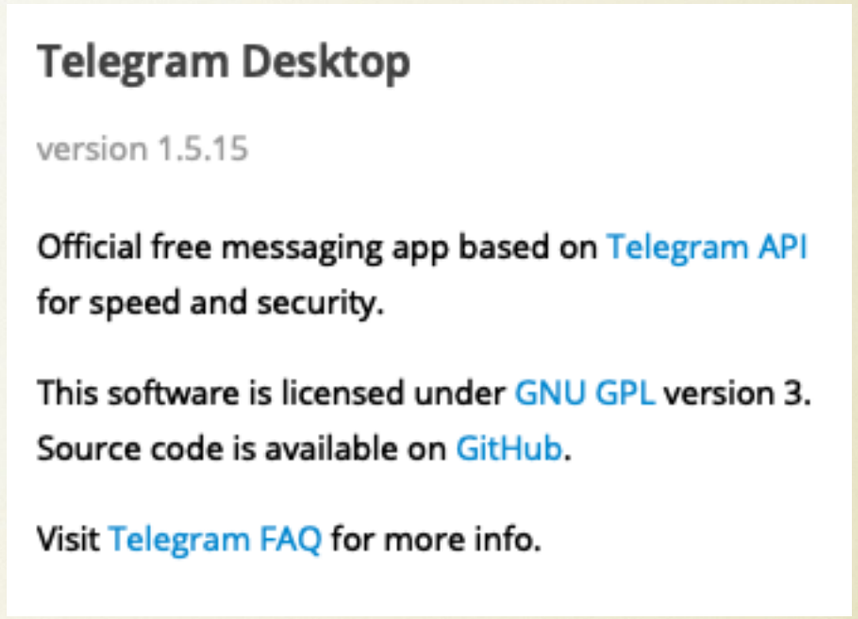
- Darf Instagram deine Fotos verkaufen?
- gewährst du Instagram hiermit eine [...] gebührenfreie, übertragbare, unterlizenzierbare, weltweite Lizenz für die Nutzung der Inhalte, die du auf dem oder durch den Dienst postest;

Quelle: https://help.instagram.com/478745558852511 (abgerufen 27.01.2017)

Das heißt: Instagram darf alles mit deinen Bildern und Texten machen, also auch sie verkaufen (Unterlizenz).

# Quiz

- Gibt es Alternativen?
- z.B. Telegramm




## F: Warum sollte ich euch vertrauen?

Wir haben nichts zu verstecken. Telegram ist offen, jeder kann den Quelltext, das Protokoll und den Entwicklerzugang (API) prüfen, um zu sehen, wie alles genau funktioniert und sich dementsprechend eine eigene Meinung bilden. Gern nehmen wir Anregungen an und freuen uns über unabhängige Sicherheitsprüfungen. Die Kontaktadresse: security@telegram.org

Quelle: FAQ, telegram.org (12.02.1019)

# Datenschutz

# Datenschutz

- Maßnahmen zum Schutz vor unerlaubter Verwendung von **personenbezogenen Daten**
- es gilt die EU-Datenschutzgrundverordnung mit:
  - Auskunftsrecht
  - Einwilligung
- das Bundesdatenschutzgesetz (BDSG)
  - Grundsätze des BDSG: Jeder Mensch muss der Verwendung seiner Daten zustimmen; Es gelten die Prinzipien Datensparsamkeit und Datenvermeidung
  - personenbezogener Daten sind:
  - besonderer Schutz gilt für folgende sensible Daten:

# Datenschutz

Technische Realisierungen zur Wahrung von Datenschutz und (Betriebs)geheimnissen

- wenn möglich Daten in Datensammlungen anonymisieren
- Zugriffschutz im Dateisystem und Netzwerk einrichten
- Verschlüsselungen von Daten

# Datenschutz

Zugriffsrechte im Dateisystem (z.B. Access Control List unter Windows)

- Wo?
  - Kontextmenü auf Dateisymbol - Register „Sicherheit“
- Einstellungen
  - Prinzip: Zugriff bei positiver Nennung und keiner negativen Nennung!
  - Rechte (vereinfacht) für User oder Gruppen: lesen, schreiben, ausführen, Vollzugriff;
  - Hinweis: evtl. Vererbung aufheben

# Übungen

1. Erkläre den Begriff Datenschutz.

2. Nenne a) drei Angaben, welche zu den personenbezogenen Daten zählen und b) drei Angaben, welche als besonders schützenswert zählen.

3. Erkläre was das Bundesdatenschutzgesetz unter Datensparsamkeit und Datenvermeidung versteht.

## Übungen

4. Welche Maßnahmen dienen den Datenschutz?

    a) Anonymisieren von Daten

    b) Daten zusätzlich auf einem USB-Stick speichern

    c) Zugriffsrechte im Dateisystem und gesicherter Login

    d) Verschlüsseln von Daten

# Übungen

5. Beurteile den Umgang mit dem Datenschutz!

   a) Darf dein Arzt deinem Klassenlehrer deine Erkrankung mitteilen?

   b) Ist es richtig, wenn du bei deiner Bank deine Adresse angeben musst.

   c) Du wirst von der Medienforschung angerufen und zu deiner Mediennutzung befragt, ist es richtig dein Alter, den Namen und die Adresse zu nennen?

   d) In Gesellschaftskunde soll jeder Schüler seine Religionszugehörigkeit in eine Liste hinter seinem Namen schreiben.

# Auswertung

# Datenschutz

Schutz personenbezogener Daten

informelle Selbstbestimmung

# Datensicherheit

Schutz vor Datenverlust

Backup

Verfügbarkeit

1. Erkläre den Begriff Datenschutz
   - Recht auf Schutz personenbezogener Daten
   - Maßnahme zum Schutz vor unerlaubter Verwendung von personenbezogenen Daten.
2. Nenne a) drei Angaben, welche zu den personenbezogenen Daten zählen und b) drei Angaben, welche als besonders schätzenswert zählen.
   a) Name, Adresse, Geburtsdatum, biometrische Daten usw.
   b) Religion, politische Meinung; genetische Daten; Daten zum Sexualleben/sexuelle Orientierung
3. Erkläre was das Bundesdatenschutzgesetz unter Datensparsamkeit und Datenvermeidung versteht.
   - Konzept der Datenverarbeitung, bei dem nur so viele personenbezogene Daten gesammelt werden, wie unbedingt notwendig sind.

4. Welche der genannten Maßnahmen dienen den Datenschutz? Nenne diese und begründe kurz deine Antwort.

   a) anonymisieren von Daten dient dem Datenschutz, weil die Daten dadurch keiner Person mehr eindeutig zugeordnet werden können.

   b) ~~Daten zusätzlich auf einem USB-Stick speichern~~

   c) Zugriffsrechte im Dateisystem und gesicherter Login dient dem Datenschutz, weil damit gewährleistet wird, dass Dritte keinen unberechtigten Zugriff auf Daten erhalten (oder erschwert wird).

   d) Verschlüsseln von Daten dient dem Datenschutz, weil dadurch Daten nur von den Empfängern gelesen werden können, welche einen Schlüssel zum dechiffrieren besitzen. Unbefugte haben also keinen Zugriff.

5. Beurteile den Umgang mit dem Datenschutz.
   a) Darf dein Arzt deinem Klassenlehrer deine Erkrankung mitteilen?
   - Nein, der Arzt besitzt kein Befugnis darüber den Gesundheitsstatus von Schülern einen anderen zu melden.

   b) Ist es richtig, wenn du bei deiner Bank deine Adresse angeben musst.
   - Ja, denn die Bank benötigt diese zum Erfüllen ihres Geschäftszweckes.

   c) Du wirst von der Medienforschung angerufen und zu deiner Mediennutzung befragt, ist es richtig dein Alter, den Namen und die Adresse zu nennen?
   - Nein, weil diese Daten zu den personenbezogenen Daten zählen und für die Befragung zur Mediennutzung irrelevant sind (Datenvermeidung).

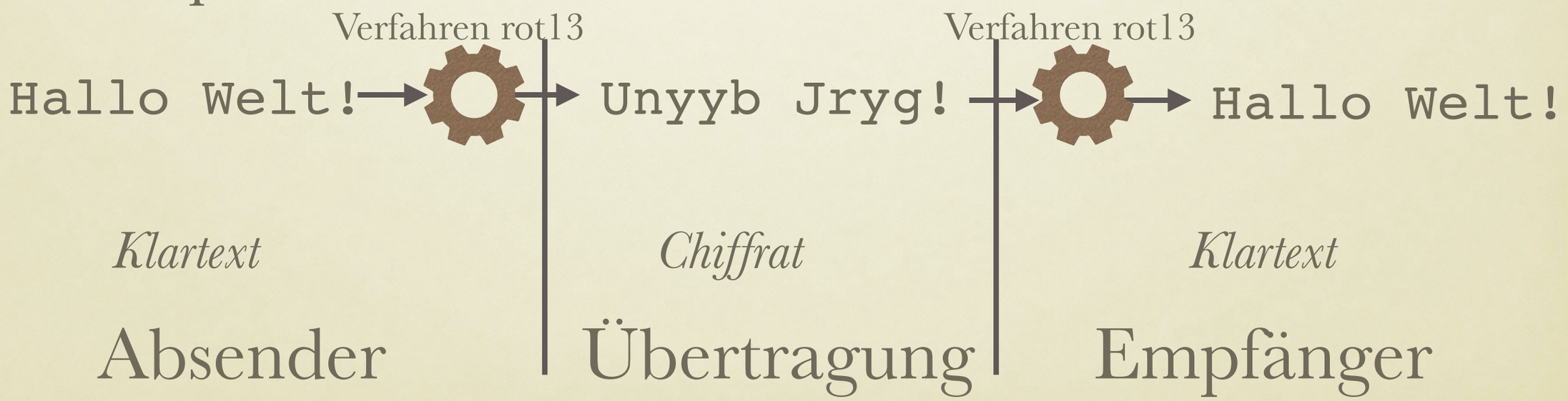
   d) In Gesellschaftskunde soll jeder Schüler seine Religionszugehörigkeit in eine Liste hinter seinem Namen schreiben.
   - Nein, weil Daten zur Religionszugehörigkeit besonders geschützt sind.

# Datenschutz durch Verschlüsselung

- Verschleierung (Cäsar-Kodierung, rot13)
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

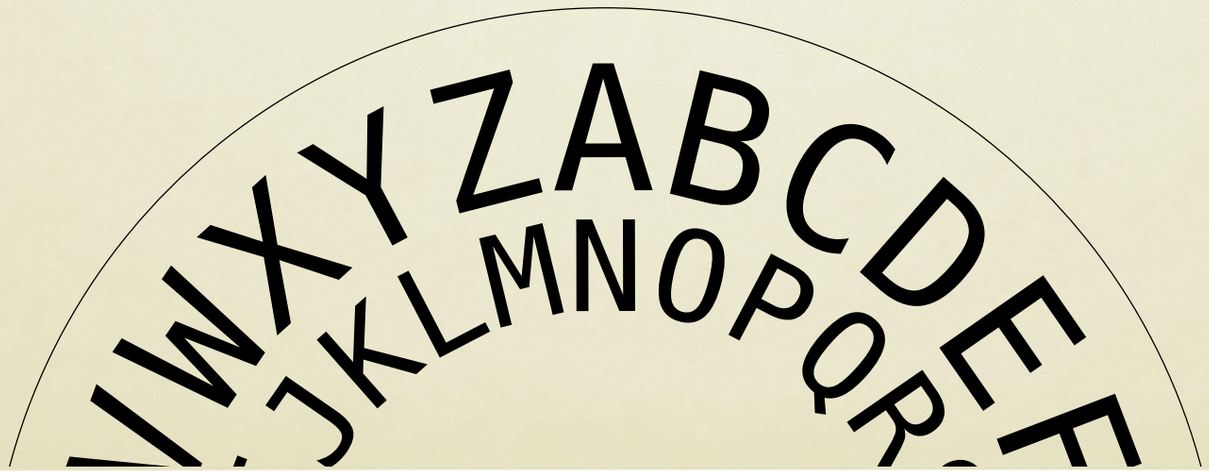
## Verschleierung

- Cäsar-Kodierung: Buchstaben werden um eine festgelegte Anzahl an Stellen verschoben.
- rot13:  Verfahren ähnlich der Cäsarkodierung, hier werden die Buchstaben um 13 Stellen verschoben. Damit erfolgt die Entschlüsselung der 26 Buchstaben durch eine nochmalige Verschiebung um 13 Stellen.
- Beispiel:



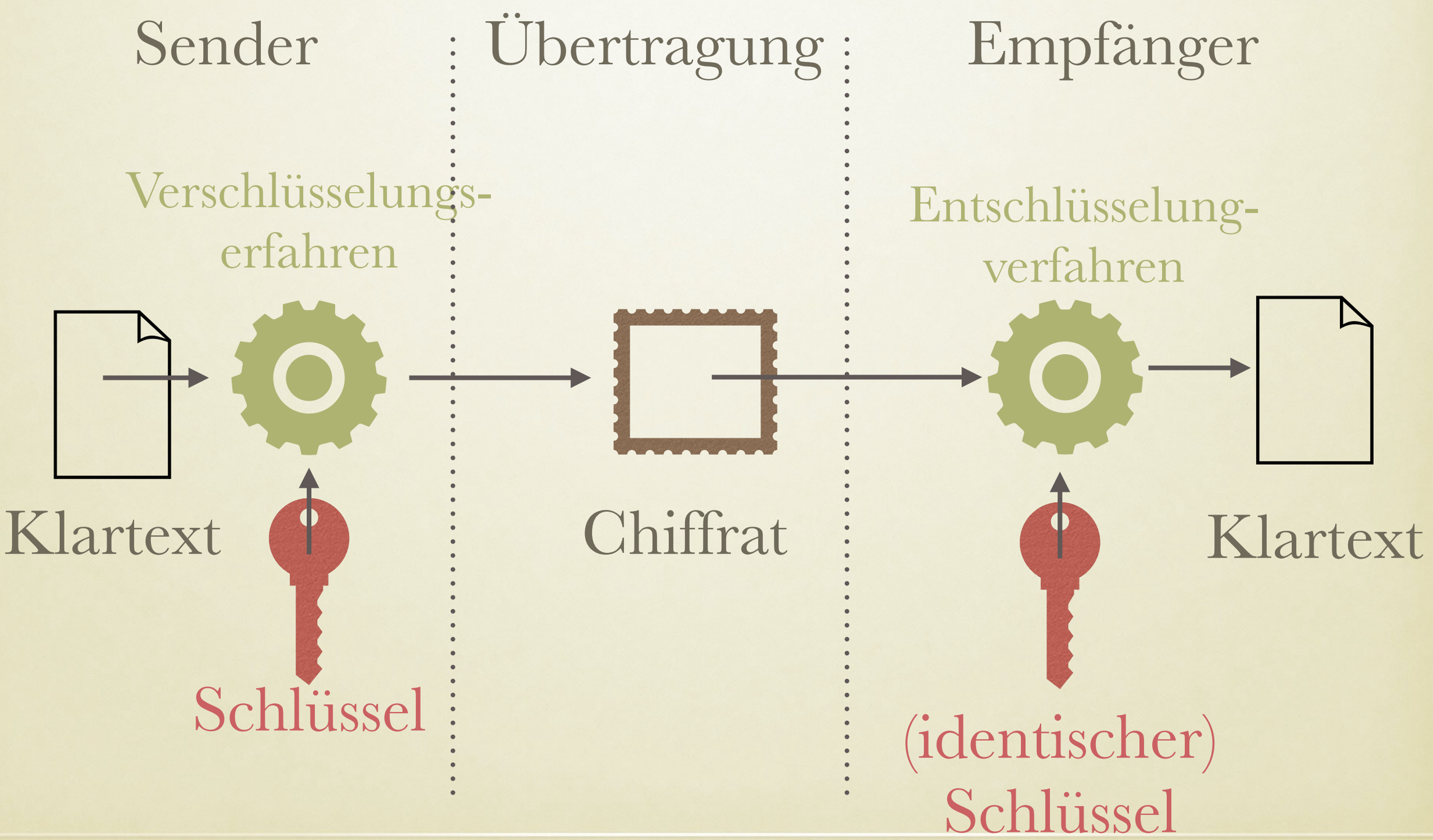
# Verschleierung rot 13 - Erkundung

1. Besuch die Webseite „rot13.com"
   - Erstelle einen kurzen Text und lasse die Textzeichen um 13 Stellen rotieren.
2. Schreibe das Ergebnis auf einen Zettel und gib diesen an deinen Nachbarn weiter.
3. Der Empfänger gibt auf der Webseite „rot13.com“ den Text ein und rotiert die Textzeichen ebenfalls um 13 Stellen.



# Symmetrische Verschlüsselung

- Prinzip:



# Symmetrisch

beispielhaftes Verfahren:

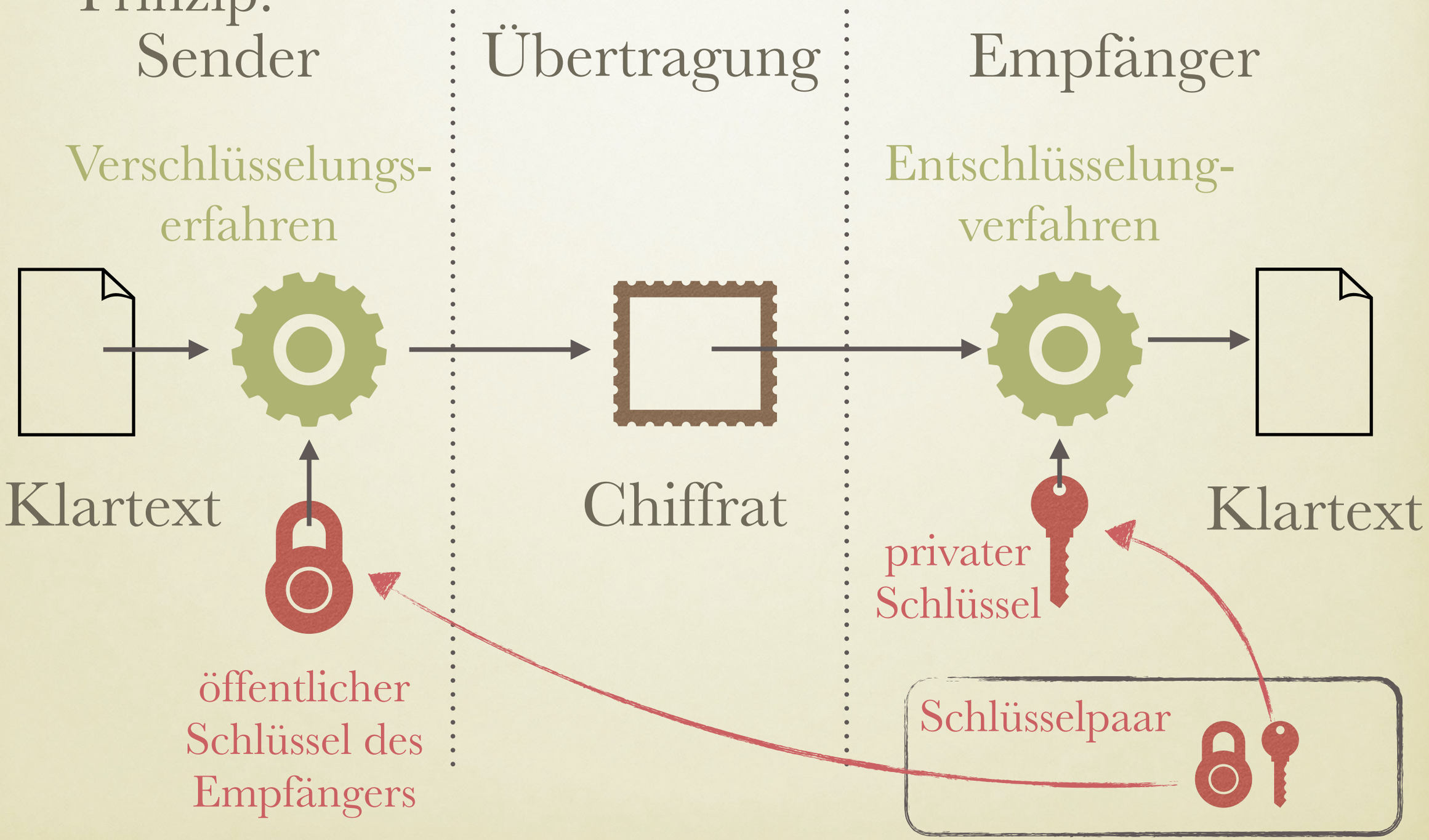
- Absender denkt sich einen Zahlen-Schlüssel aus, z.B. 1450
- der Schlüssel muss geheim zum Empfänger gelangen
- der Text wird folgendermaßen überführt:
  - Buchstaben werden um die jeweilige Stelle des Schlüssels in Wiederholung verschoben, Groß- und Kleinschreibung bleibt erhalten Zahlen und Leerzeichen werden nicht verändert.
  - Ist der Schlüssel beendet, wird er wiederholt.

Bsp.:

```
Hallo Welt!
1450145014 5
Idqlp Bemx!
```

## asymmetrische Verschlüsselung

- Prinzip:



## asymmetrische Verschlüsselung

- Anwendung:
  - Email-Verschlüsselung
  - Sichere Webseiten (Onlinebanking, Onlineshop)

# Vergleich symmetrische und asymmetrische Verschlüsselung

| Eigenschaft \ Verfahren | symmetrisch | asymmetrisch |
|---|---|---|
| **rechenintensiv / langsam** | | |
| **lösbar** | | |
| **Angriff** | | |
| **Bedingung für ein sicheres Verfahren** | | |
| **Signieren (Nachweis des Absenders)** | | |

# Vergleich symmetrische und asymmetrische Verschlüsselung

| Eigenschaft \ Verfahren | **symmetrisch** | **asymmetrisch** |
|---|---|---|
| **rechenintensiv / langsam** | nein | ja |
| **lösbar** | bei Wiederholungen des Schlüssels | bisher nicht |
| **Angriff** | Abfangen oder lösen des Schlüssels | man-in-the-middle (Angreifer gibt vor der Empfänger zu sein) |
| **Bedingung für ein sicheres Verfahren** | Geheimhalten des Schlüssels, Schlüssel regelmäßig ändern | Sicherstellen, das der öffentliche Schlüssel wirklich zum Empfänger gehört |
| **Signieren (Nachweis des Absenders)** | nein | ja |

## weitere Verfahren

- Prüfsumme:
  - Daten können mit Prüfsummen überprüft oder fälschungssicher als Signatur übertragen werden.
  - bekannte Verfahren: md5, Quersumme
  - einfaches Beispiel: (Quersumme der Textzeichen, a=1, b=2 usw. Großbuchstaben + 26)

    Hallo ≙ 34 + 1 + 12 +12  + 15 = 74
    Der Text „Hallo“ wird mit der Prüfsumme „74“ übertragen, der Empfänger kann dann überprüfen ob die Übertragung fehlerfrei war.

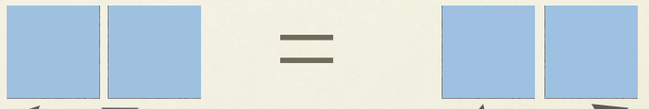
## Übung Prüfsumme

- Um die Übertragung von fünf ganzen Zahlen abzusichern soll als sechste Zahl zusätzlich deren Quersumme übermittelt werden.
- Berechne die Quersumme der folgenden Zahlenreihen:

a) 10:11:45:22:87:[ ]

b) 223:11:12:9:5:[ ]

## weitere Verfahren

- Steganographie:
  - (unverschlüsselte) Daten werden unauffällig zum Empfänger transportiert. Z.B. In digitalen Bilddaten im jeweils letzten Bit eines Bildpunktes versteckt. (Strickmuster mit Bedeutung, tätowierte Kopfhaut usw.)
- Beispiel: 101011…+  =

9FC1E0
9[1111]C[0001]E[0000]

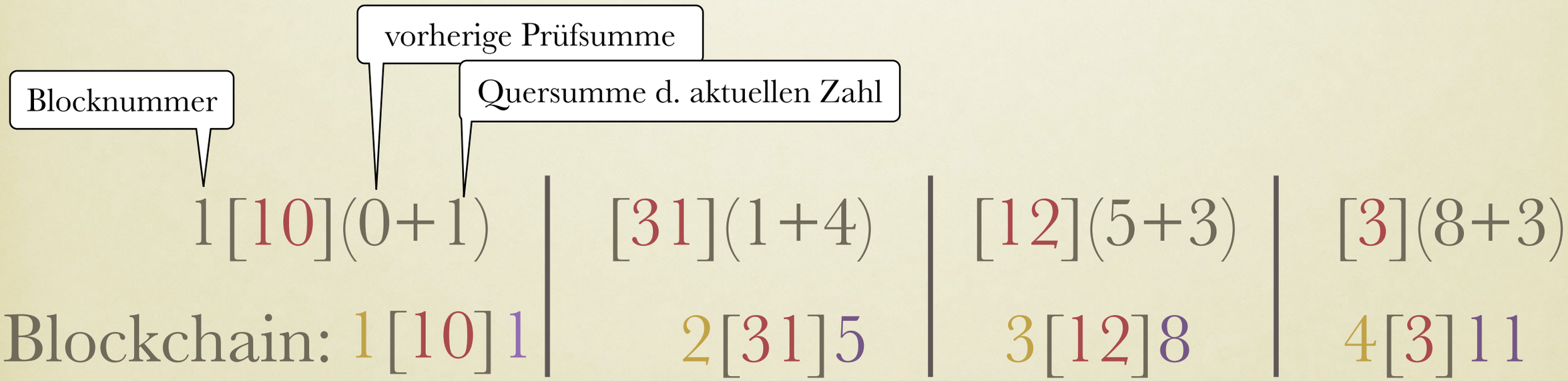
9FC0E1
9[1111]C[0000]E[0001]

9EC1E1
9[1110]C[0001]E[0001]

- Problem: Verfahren muss geheim gehalten werden!

## weitere Verfahren

- Blockchain:
  - kontinuierlich erweiterbare Kette von kryptografisch gesicherten Datensätzen, die nachträglich nicht geändert werden kann.
  - einfaches Beispiel: Übertragung von mehreren ■ Blöcken mit ■ Zahlen und deren Absicherung über ■ Prüfsummen



# Datensicherheit

- Maßnahmen zum Vermeiden von Datenverlusten und dem Ausfall der Datenverfügbarkeit
- Gründe für einen Datenverlust (Aufgabe: Nenne Gründe für einen Datenverlust - Sortierung nach:)
  - Hardware
  - Benutzerfehler
  - Schadsoftware

| Hardware | Benutzerfehler | Software |
| --- | --- | --- |
| | | |
| | | |
| | | |

# Datensicherheit

- Maßnahmen, um Datenverluste zu vermeiden (Erkläre, wie du deine Daten vor Verlust schützen kannst.)
- Bsp. Organisatorisch:
- Bsp. Technisch:

Beispiel veracrypt
https://www.veracrypt.fr/en/Downloads.html

- Verschlüsselung von Dateisystemen (z.B. Komplexer USB-Stick) oder Erstellung von verschlüsselten Speicherplatz in einer Datei
- es wird z.B. mit AES symmetrisch verschlüsselt