

Ist meine Kaffeemaschine ein Computer?

Ziele

Dieser Kurs soll die folgenden Fragen beantworten:

- Tag 1: Was ist ein Computer?
- Tag 2: Was ist das Internet?

Was ist ein Computer?

- Was ist ein Computer?
- Computer-Architektur
- Daten-Kodierung
- Eingebettete Systeme (Embedded Devices)
- Was ist ein Algorithmus?

Welches von diesen Geräten ist ein Computer?

- Notebook
- Smartphone
- Sprachassistenten (Alexa, HomePod, ...)
- Raspberry Pi
- Waschmaschine
- Kaffeemaschine
- Auto

Was ist ein Computer?

Wikipedia

Ein Computer [...] ist ein Gerät, das mittels programmierbarer Rechenvorschriften Daten verarbeitet.

Computer sind heute in allen Bereichen des täglichen Lebens vorzufinden, meistens in spezialisierten Varianten, die auf einen vorliegenden Anwendungszweck zugeschnitten sind. So dienen integrierte Kleinstcomputer [...] zur Steuerung von Alltagsgeräten wie Waschmaschinen [...]; in modernen Automobilen dienen sie [...] zur Anzeige von Fahrdaten und steuern in „Fahrassistenten“ diverse Manöver selbst.

Was ist ein Computer?

Fast jedes moderne Gerät beinhaltet mindestens einen Computer in Form eines integrierten Kleinstcomputer (Embedded Device)

Computer-Architektur

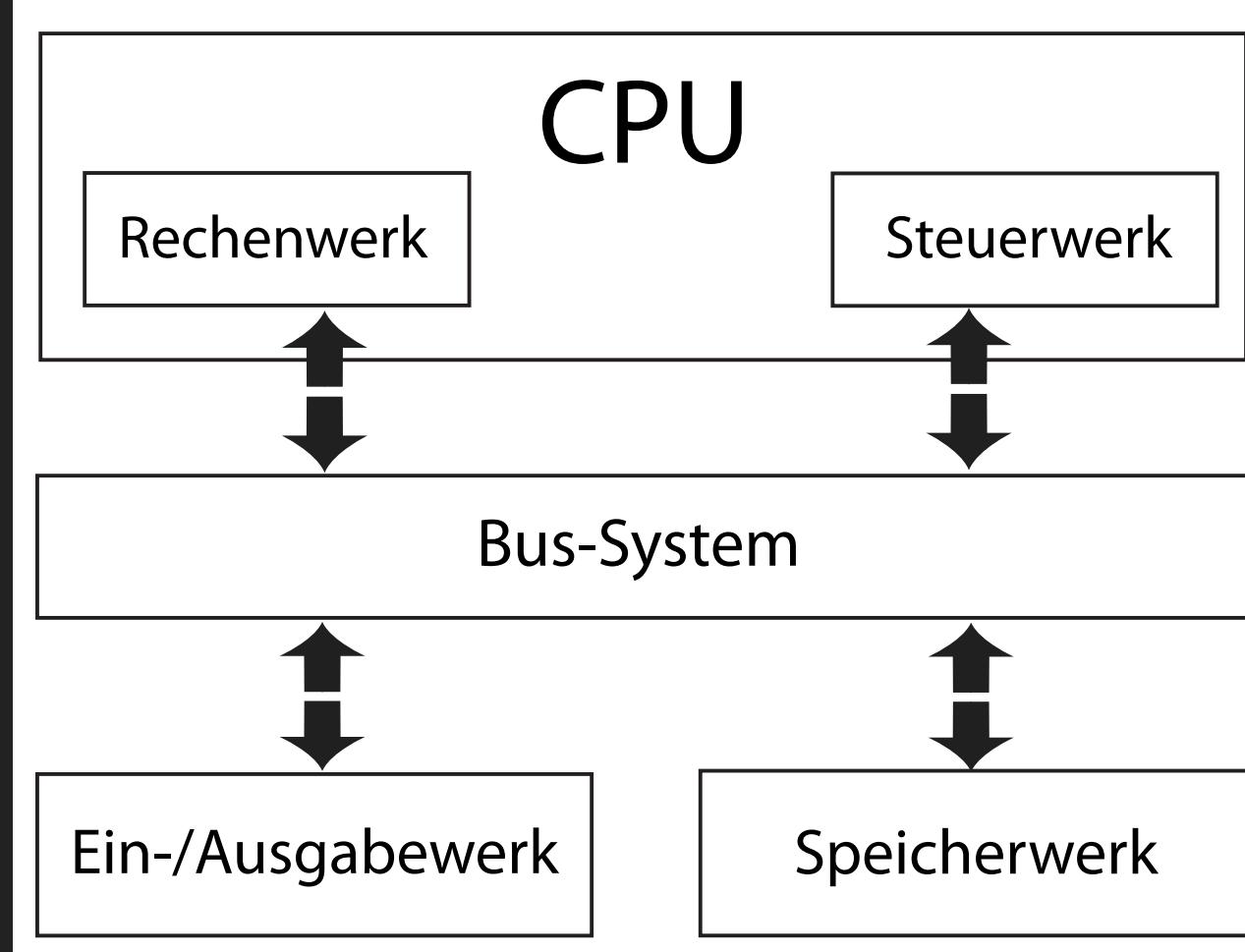
Fast alle aktuellen Computer verwenden die [Von-Neumann-Architektur](#)

- Idee: Programme und Daten werden im Speicher abgelegt

Von-Neumann-Architektur

- CPU
 - Rechenwerk (ALU)
 - Steuerwerk (Control Unit)
- Bus System
 - Speicherwerk (RAM, Festplatte)
 - I/O Unit (Tastatur, Bildschirm)

Grafik: Wikipedia





Central Processing Unit (CPU)
Intel Core i7, AMD Ryzen 9, ...
Quelle: [Wikimedia](#)



Arbeitsspeicher (RAM)
Typische Größen: 8GB, 16GB
GB: Gigabyte
Quelle: [Wikimedia](#)



Solid State Disk (SSD)

Typische Größen: 512GB, 1TB, 2TB
TB: Terrabyte (1000GB)

Quelle: [Wikimedia](#)



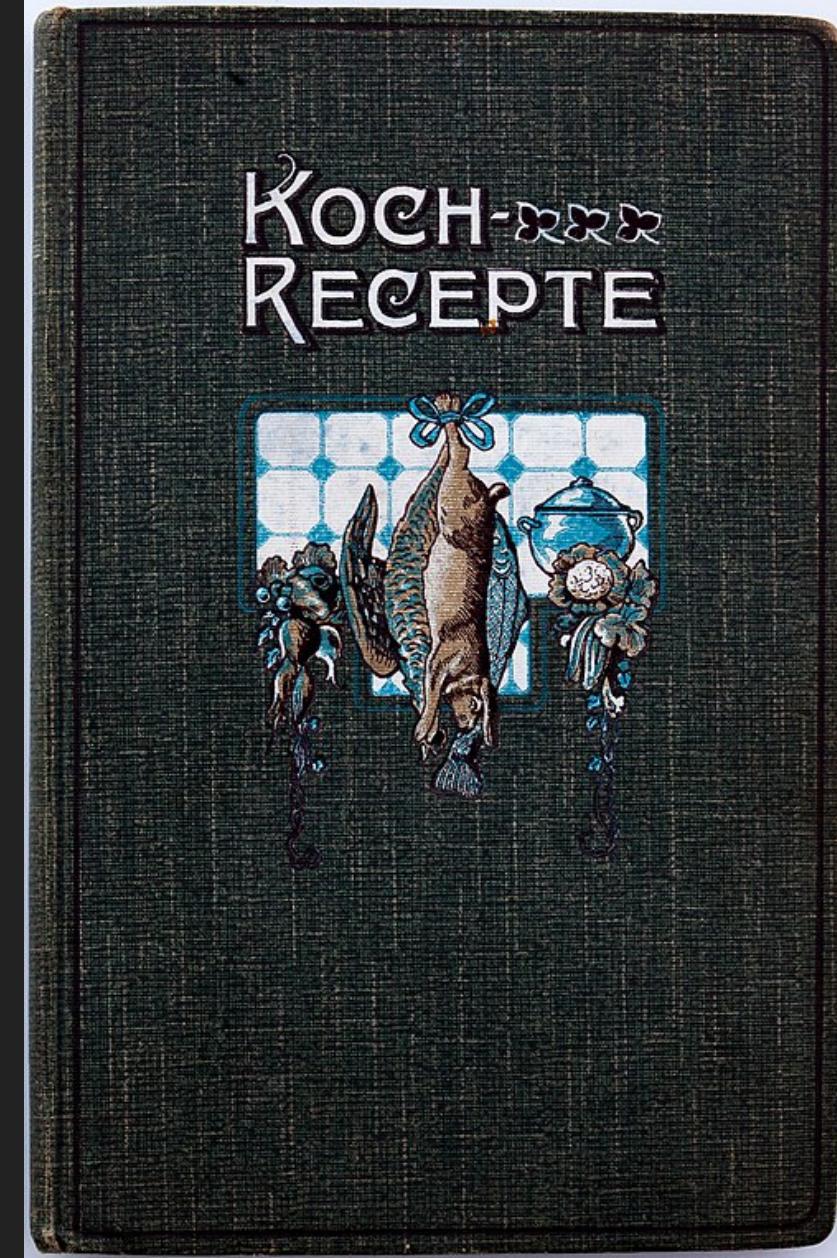
Hard Disk (HDD)
langsamer als SSDs, aber günstiger
Typische Größen: 1TB, 2TB, 4TB
Quelle: [Wikimedia](#)

Wie funktioniert ein Computer?

Was ist ein Programm?

- lineare Liste von Befehlen
- auf dem persistenten Speicher (SSD, HDD) abgelegt
- verarbeiten Daten

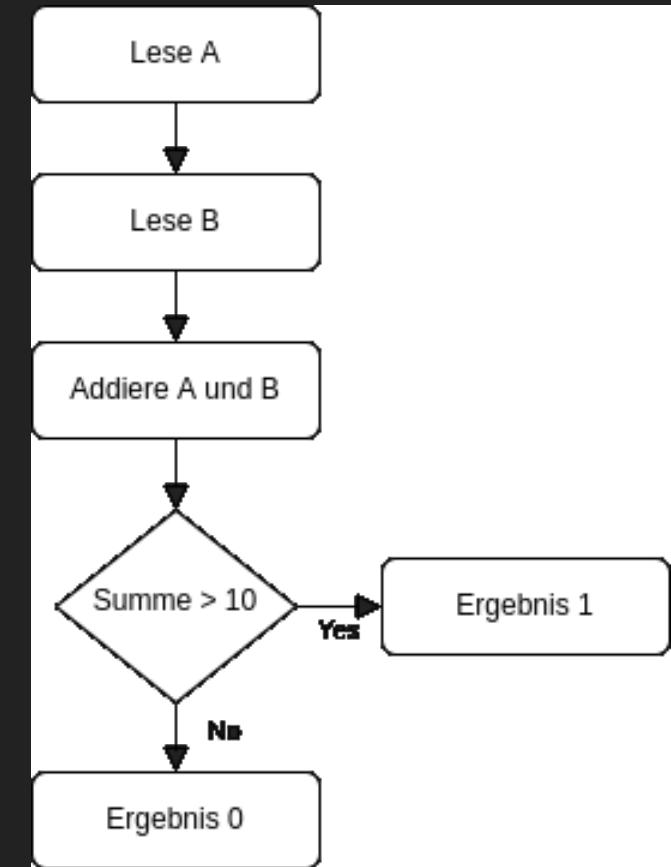
Grafik: Wikimedia



Wie funktioniert ein Computer?

Wie wird ein Programm ausgeführt?

- Befehle werden ins RAM geladen
- CPU hat einen lokalen Status (Register, ...)
- Befehle können Daten und CPU Status ändern
- Befehle werden linear abgearbeitet
- Mit Sprungbefehlen können Entscheidungen und Schleifen realisiert werden
- einzelne Befehle haben eine geringe Komplexität (Rechnenoperationen, Vergleich, Sprünge)



Daten-Kodierung

Binär

- heutige Computer kennen nur 0 und 1 (kein Strom, Strom)
- alle Daten und Programme müssen als 0 und 1 dargestellt werden

Daten müssen Binär kodiert werden

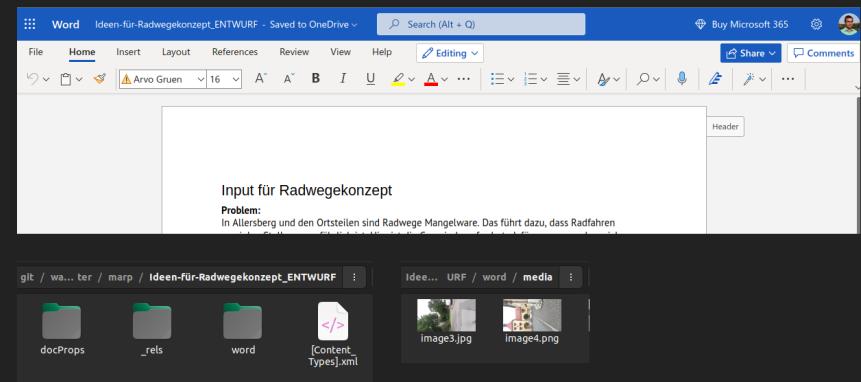
- Nachricht (Syntax): Folge von 0en und 1en
- Information (Semantik): Bedeutung der Nachricht
- Daten: Nachricht + Information

Daten Darstellung und Verarbeitung

- Programme
 - verarbeiten Daten (anzeigen, manipulieren)
 - interpretieren Daten
- die Darstellung von Daten in Programmen
 - ist auf einen bestimmten Anwendungsfall ausgerichtet
 - kann unvollständig sein

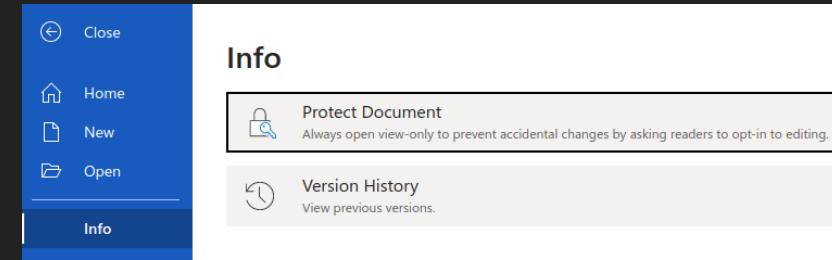
Exkurs: Word Dokumente

- Word-Dokumente ([docx](#)) sind Zip-Dateien
- Experiment: docx in zip umbenennen
- Resultat: Ordnerstruktur mit xml, ...



Exkurs: Word Dokumente

- Dokumente können mehr beinhalten als auf den ersten Blick ersichtlich ist
- Word Dokumente beinhalten:
 - die Änderungshistorie
 - Metadaten (Author)



Zahlensysteme

Dezimalsystem

- $123_{10} = 1 * 100 + 2 * 10 + 3 * 1$
- Wertigkeit der Stellen: 10^i : $10^0 = 1, 10^1 = 10, 10^2 = 100, \dots$

Zahlensysteme

Dualsystem

- $101_2 = 1 * 4 + 0 * 2 + 1 * 1 = 5_{10}$
- Wertigkeit der Stellen: 2^i : $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, \dots$

Hexadetimalsystem

- $10_{16} = 1 * 16 + 0 * 1 = 16_{10}, AF_{16} = 10 * 16 + 15 * 1 = 175_{10}$
- Wertigkeit der Stellen: 16^i : $16^0 = 1, 16^1 = 16, 16^2 = 256, \dots$

Zahlensysteme

Hexadezimaldarstellung von Binärdaten

- maximaler Wert einer 4-stelligen Binärzahl: $8 + 4 + 2 + 1 = 15$
- maximaler Wert einer 1-stelligen Hexadezimalzahl: $F_{16} = 15$
- 4 Zeichen binär ($XXXX_2$) = 1 Zeichen hexadezimal
- Binär-Daten lassen sich kompakt Hexadezimal darstellen:
 - $1100_2 = 12_{10} = A_{16}$
 - $11000101_2 = 1100\ 0101 = A5_{16}$
 - 1 Byte = 8 Bit ($XX_{16}, XXXX.XXXX_2$)

Zahlendarstellung im Computer

Zweierkomplement

- Zahlenraum: $-2^{n-1}, \dots, 0, \dots -2^{n-1}$
- 8bit: -127...127
- 32bit: -4.294.967.295...4.294.967.295
- Berechnung
 - Positive Zahlen: Binärdarstellung
 - Negative Zahlen: Binärdarstellung invertieren und 1 addieren
 - $-4 = 0000\ 0100$
 - invertiert: $1111\ 1011$
 - 1 addieren: $1111\ 1100$

Gleitkommazahlen IEEE 754

- Gleitkommazahlen (z.B. 3,14) müssen als Binärmuster darstellt werden
- Standard: IEEE 754:
 - $x = s m 2^e$
 - Vorzeichen s (1 Bit)
 - Mantisse m (p Bits)
 - Exponent e (r Bits)
- 32 Bit Darstellung: $3,14 = 0 \ 2^1 \ 1.5700000524520874 = 0\ 1000.0000\ 100.1000.1111.0101.1100.0011$
- Dargestellte Zahl: 3.1400001049041748046875

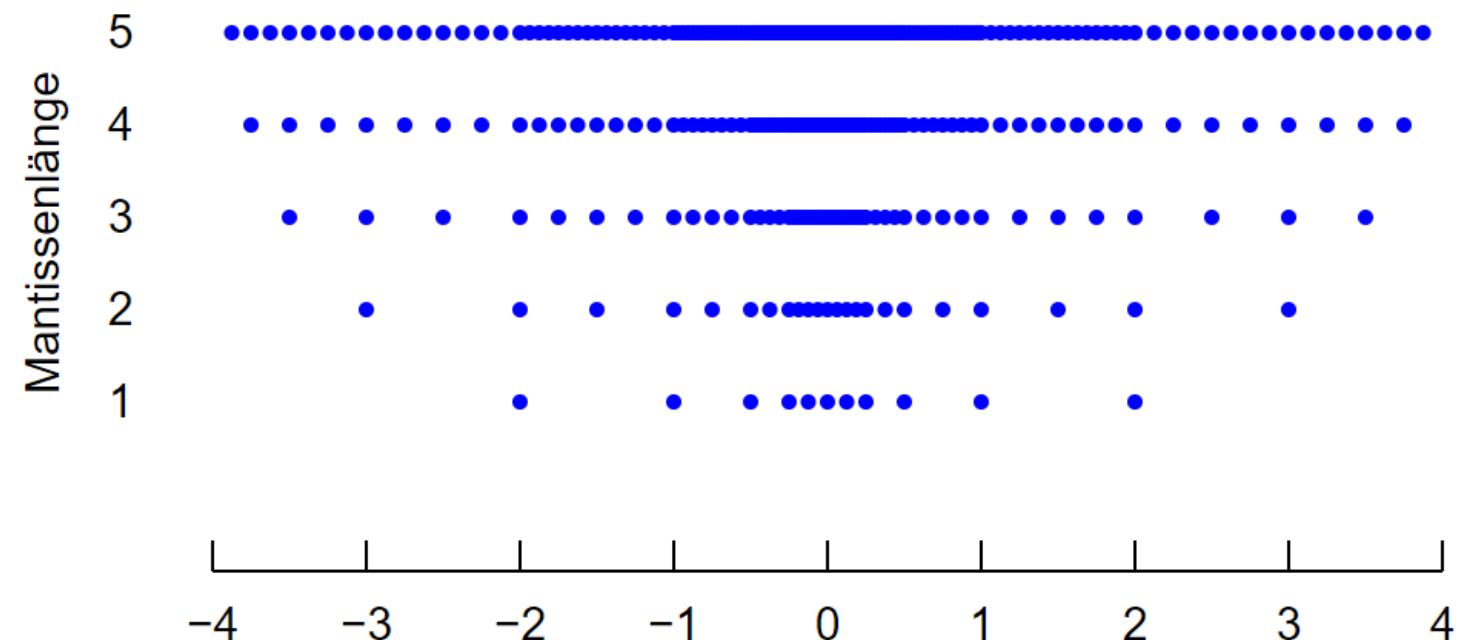
IEEE_754

Nicht alle Zahlen
darstellbar.

Rundungsfehler!

Grafik: Wikimedia

Exakt darstellbare Gleitkommazahlen



Texte im Computer

- Kodierung pro Zeichen
- einfachste Kodierung: [ASCII](#)
 - ein Zeichen pro Byte, sehr kleiner Zeichenraum
- aktueller Standard: [UTF8](#)
 - variable Zeichenlänge, (fast) alle Zeichen darstellbar

Exkurs: Zeichenkodierung

- Text: Hallo, Welt!
 - ASCII: 48 61 6c 6c 6f 2c 20 57 65 6c 74 21
 - UTF-8: 48 61 6c 6c 6f 2c 20 57 65 6c 74 21
 - UTF-16: 0048 0061 006c 006c 006f 002c 0020 0057 0065 006c 0074 0021
- Zeichen: 龙
 - ASCII: Nicht darstellbar
 - UTF-8: e2 bb b0
 - UTF-16: 2ef0
- Was ist das dritte Zeichen in einem UTF-8 kodierten Text?

Bilder im Computer

- Bilder werden als Pixel-Raster gespeichert
- eine Farbe pro Pixel
- verschiedene Farbkodierungen, z.B. **RGBA**
- einfachste Kodierung: **BMP**
- übliche Formate:
 - jpg (verlustbehaftet, Fotos)
 - png (verlustfrei, Internet)

Grafik: Pohlig.de

BMP-Datei		
Offset (dez)	Daten (hex)	Bedeutung
0000	42 4D	Datei-Identifikation ("BM")
0002	5E 04 00 00	Dateilänge (1118 Bytes)
0006	00 00 00 00	Reserviert
0010	36 04 00 00	Zeiger auf Pixeldaten (Offset 1078)
0014	28 00 00 00	Headergröße (40 = 28 ₁₆ Bytes)
0018	06 00 00 00	Bildbreite (6 Pixel)
0022	05 00 00 00	Bildhöhe (5 Pixel)
0026	01 00	Anzahl Ebenen (1)
0028	08 00	Bits pro Pixel (8)
0030	00 00 00 00	Kompression (0, unkomprimiert)
0034	28 00 00 00	Größe der Pixeldaten (40 Bytes)
0038	C4 0E 00 00	X-Auflösung (75 dpi)
0042	C4 0E 00 00	Y-Auflösung (75 dpi)
0046	00 00 00 00	Anzahl genutzter Farben (ignoriert)
0050	00 00 00 00	Anzahl wichtiger Farben (ignoriert)
0054	00 00 00 00	Farbe 0 (schwarz)
0058	00 00 80 00	Farbe 1 (mittleres rot)
0062	00 80 00 00	Farbe 2 (mittleres grün)
...
1074	FF FF FF 00	Farbe 255 (weiß)
1078	C2 C2 C2 C2 C2 C2 00 00	Unterste = 5. Pixelzeile
1086	C2 00 FF 00 FF C2 00 00	4. Pixelzeile
1092	C2 FF 00 FF 00 C2 00 00	3. Pixelzeile
1100	C2 00 FF 00 FF C2 00 00	2. Pixelzeile
1008	C2 C2 C2 C2 C2 C2 00 00	1. Pixelzeile

Exkurs: Bilder

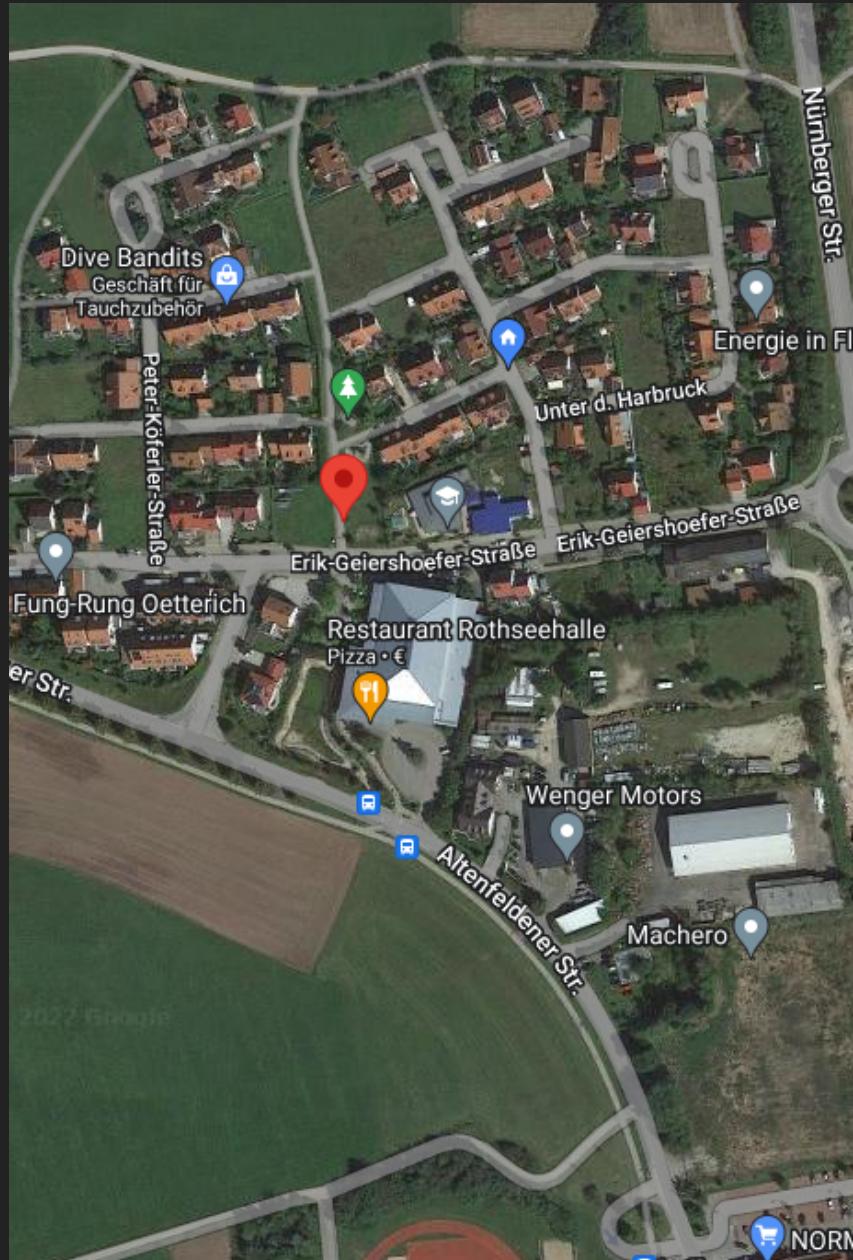
- Metadaten

```
...  
exif:DateTime: 2020:08:05 13:17:10  
...  
exif:GPSLatitude: 49/1, 15/1, 3560/100  
exif:GPSLatitudeRef: N  
exif:GPSLongitude: 11/1, 13/1, 3996/100  
exif:GPSLongitudeRef: E  
...  
exif:Model: iPhone 11
```



Exkurs: Bilder

- Ort: N 49° 15' 35.60 E 11° 13' 39.96
- Aufnahmezeit: 05.08.2020 13:17:10
- Gerät: iPhone 11
- Jedes Foto-Posting ins Internet (Facebook, Strava, ..) verrät auch den genauen Standort



Exkurs: PDF

- Google: site:vhs-roth.de filetype:PDF
- Hygiene- und Präventionskonzept für vhs-Kurse
- Metadaten:

...
Author : Zargaoui, Karin
Creator : Acrobat PDFMaker 17 für Word
...
CreationDate : Wed Aug 26 09:47:59 2020 CEST



Hygiene- und Präventionskonzept für vhs bei der vhs im Landkreis Roth – gültig ab 22.07.2020

Das Konzept entspricht in Gänze den Hygienevorschriften des Bayerischen Staates. Kursspezifische Regularien ergänzen. Im Rahmen der vhs im Landkreis Roth sind Hygieneanforderungen zur Vermeidung von Covid-19-Infektionen zwingend einzuhalten.

Vor Kursantritt und –beginn

Die Teilnehmenden sind darauf hinzuweisen, dass sie bei Vorliegen von Krankheitssymptomen oder Kontakt mit Corona-Infizierten nicht am Kurs teilnehmen. Sollte eine Teilnahme trotzdem stattfinden, ist der Kursleiter ein Kursteilnehmer/eine Kursteilnehmerin während der Durchführung zu informieren. Hier ist die Eigenverantwortung der Kursteilnehmenden unerlässlich. Kursleitenden/Dozent*innen gefordert.

Personen mit Erkältungssymptomen sind nicht zugelassen. Bei den Kursen und Seminaren in allen Fachbereichen ist der Mindestabstand von 1,5 m bzw. 1,5 m², bei Führungen im Innenbereich 20 m zwingend einzuhalten, andernfalls ist eine Abseuchung zu erwarten.

Was ist ein Algorithmus?

Wikipedia:

Ein Algorithmus ist eine eindeutige Handlungsvorschrift zur Lösung eines Problems oder einer Klasse von Problemen.

Eigenschaften eines Algorithmus

- endlich beschreibbar (Finitheit)
- jeder Schritt muss (eindeutig) ausführbar sein (Ausführbarkeit)
- darf nur endlich viel Speicher verwenden (dynamische Finitheit)
- darf nur endlich viele Schritte benötigen (Terminierung)
- muss unter denselben Voraussetzungen das gleiche Ergebnis liefern (Determiniertheit)
- der nächste Schritt muss zu jedem Zeitpunkt eindeutig sein (Determinismus)

Algorithmus in den Medien

- algorithmische Darstellung von Inhalten (z.B. Posts, Filme, ...)
- Darstellung wird auf bestimmte Ziele optimiert
 - Optimierung auf Unternehmensziel (nicht Benutzerziele)

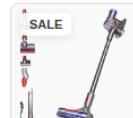
Ungefähr 49.200.000 Ergebnisse (0,46 Sekunden)

Anzeige · <https://www.dyson.de/> ▾**Staubsauger kaufen - Erleben Sie die Dyson Produkte**

Für die Reinigung des gesamten Zuhause. **Staubsauger** von Dyson jetzt entdecken!
Hygienische Behälterentleerung ohne Filter und Flexi-Düse für...



Anzeigen · Einkaufen



Dyson V8

Absolute...

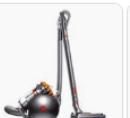
379,00 € 399,-€

Dyson Germany

Kostenloser ...

Geschenk

Von Google



Dyson Big Ball

Multifloor 2 ...

299,00 €

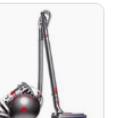
Dyson Germany

Kostenloser ...

Energie: A

★★★★★ (829)

Von Google



Dyson Cinetic

Big Ball...

499,00 €

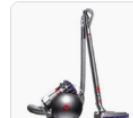
Dyson Germany

Kostenloser ...

Energie: A

★★★★★ (438)

Von Google



Dyson Big Ball

Parquet 2...

349,00 €

Dyson Germany

Kostenloser ...

★★★★★ (776)

Von Google



Dyson V15

Detect Absolu...

709,00 €

Dyson Germany

Kostenloser ...

★★★★★ (1k+)

Von Google



Dyson V8 Extra

kabelloser...

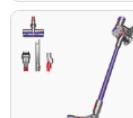
349,00 €

Dyson Germany

Kostenloser ...

★★★★★ (2k+)

Von Google



Dyson V8 Origin

kabelloser...

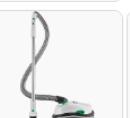
319,00 €

Dyson Germany

Kostenloser ...

★★★★★ (996)

Von Google



VT300

Bodenstaubs...

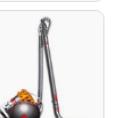
869,00 €

Vorwerk

Kostenloser ...

★★★★★ (617)

Von smec



Dyson Cinetic

Big Ball...

399,00 €

Dyson Germany

Kostenloser ...

★★★★★ (221)

Von Google

<https://www.amazon.de/staubsauger/k=staubsauger> ▾**Suchergebnis auf Amazon.de für: staubsauger**

Siemens Staubsauger mit Beutel Q5.0 extreme silencePower VSQ5X1230, Bodenstaubsauger, ideal für Allergiker, Hygiene-Filter, starke Saugleistung, Bodendüse für ...

Ähnliche Fragen

Was ist momentan der beste Staubsauger?



Welchen Staubsauger empfiehlt Stiftung Warentest?



Welcher Staubsauger ist Testsieger 2021?



Welcher Staubsauger ist besser als Dyson?



Feedback geben

<https://www.mediamarkt.de/category/staubsauger-re...> ▾**Staubsauger & Reiniger im Onlineshop bestellen**

Staubsauger & Reiniger bei MediaMarkt: Jetzt Staubsauger mit & ohne Beutel, Akkusauger, Fenstersauger, Hochdruckreiniger & mehr entdecken.

Ungefähr 49.200.000 Ergebnisse (0,46 Sekunden)

Anzeige · <https://www.dyson.de/> ▾**Staubsauger kaufen - Erleben Sie die Dyson Produkte**

Für die Reinigung des gesamten Zuhause. **Staubsauger** von Dyson jetzt entdecken! Hygienische Behälterentleerung ohne Filter und Flexi-Düse für...

**Dyson Akkustaubsauger**

Konstant hohe Saugkraft zur Reinigung des gesamten Zuhause

Staubsauger Verleich

Welcher Dyson Staubsauger ist für Sie der Richtige?

Anzeige · <https://www.vorwerk.com/vorwerk> ▾**Kobold Staubsauger auf Platz 1 - Testsieger im Doppelpack**

Bis 03.10. dein **Staubsauger**-Wunschset auswählen & bis zu 315 € sparen. Jetzt entdecken!

Anzeige · <https://www.bosch-home.com/> ▾**Bodenstaubsauger von Bosch - Starke Saugleistung**

Automatische Leistungsanpassung je nach Bodenart dank Auto-Stufe - Bosch Unlimited Gen2.

Anzeige · <https://www.aeg.de/> ▾**Staubsauger - AEG Staubsauger**

Innovative Cyclone-Technologie für optimierten Luftstrom bietet eine hohe Saugleistung

<https://www.amazon.de> › staubsauger › k=staubsauger**Suchergebnis auf Amazon.de für: staubsauger**

Siemens Staubsauger mit Beutel Q5.0 extreme silencePower VSQ5X1230, Bodenstaubsauger, ideal für Allergiker, Hygiene-Filter, starke Saugleistung, Bodendüse für ...

Ähnliche Fragen[Was ist momentan der beste Staubsauger?](#)[Welchen Staubsauger empfiehlt Stiftung Warentest?](#)[Welcher Staubsauger ist Testsieger 2021?](#)[Welcher Staubsauger ist besser als Dyson?](#)

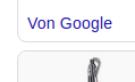
Feedback geben

<https://www.mediamarkt.de> › category › staubsauger-re...**Staubsauger & Reiniger im Onlineshop bestellen**

Staubsauger & Reiniger bei MediaMarkt: Jetzt **Staubsauger** mit & ohne Beutel, Akku staubsauger, Fensterstaubsauger, Hochdruckreiniger & mehr entdecken

Anzeigen · Einkaufen

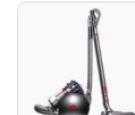
Dyson V8 Absolute...
379,00 € 399,-
Dyson Germany
Kostenloser ...
Geschenk



Dyson Big Ball Multifloor 2 ...
299,00 €
Dyson Germany
Kostenloser ...
★ ★ ★ ★ (829)
Von Google



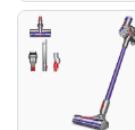
Dyson Cinetic Big Ball...
499,00 €
Dyson Germany
Kostenloser ...
Energie: A
★ ★ ★ ★ (438)
Von Google



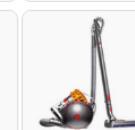
Dyson V15 Detect Absolu...
709,00 €
Dyson Germany
Kostenloser ...
★ ★ ★ ★ (776)
Von Google



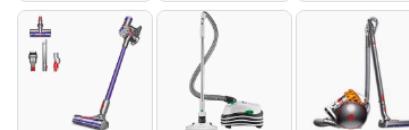
Dyson V8 Extra kabelloser...
349,00 €
Dyson Germany
Kostenloser ...
★ ★ ★ ★ (2k+)
Von Google



Dyson V8 Origin kabelloser...
319,00 €
Dyson Germany
Kostenloser ...
★ ★ ★ ★ (996)
Von Google



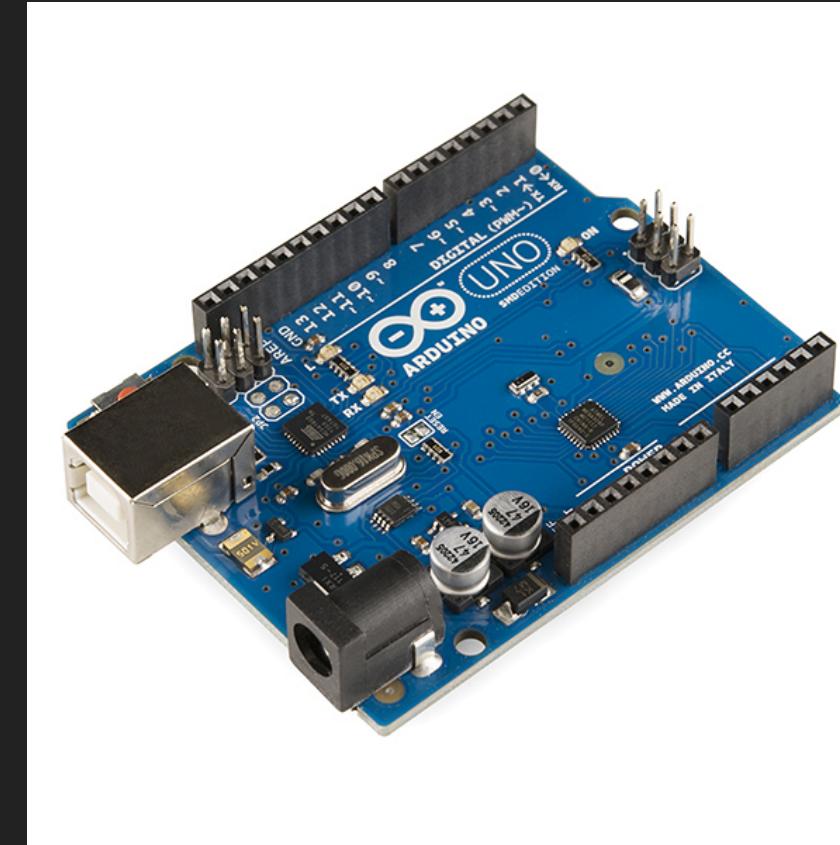
VT300 Bodenstaubsa...
869,00 €
Vorwerk
Kostenloser ...
★ ★ ★ ★ (617)
Von smec



Dyson Cinetic Big Ball...
399,00 €
Dyson Germany
Kostenloser ...
★ ★ ★ ★ (221)
Von Google

Eingebettetes System (Embedded Device)

- (kompakter) (Einplatinen-) Computer
- Spezielle Aufgabe
- Eingabe sind häufig Sensoren (Temperatur, ..., Radar)
- Ausgabe sind häufig Aktoren (Motoren, ...)



Grafik: Wikimedia

Ist meine Kaffeemaschine ein Computer? Ja!

- Ein eingebettetes System steuert die mechanischen und elektrischen Komponenten, Sensoren (Temperatur, ...) sind die Eingabe
- Die Kaffee-Rezepte ist als Programme in einem eingebauten Speicher abgelegt



Grafik: Wikimedia

Smarte Geräte

- Vorteile:
 - benutzerfreundlicher
 - fortgeschrittene Funktionen
- Nachteile:
 - Geräte "im Internet" (WLAN) brauchen Updates
 - Smarte Geräte sind häufig "Backends" angewiesen

NOT SO SMART HOME

Dampf statt Mikrowelle: Update stürzt Backofen von AEG in Identitätskrise

Hersteller Electrolux muss in den Benelux-Staaten nun Techniker zur Behebung ausschicken

21. März 2022, 13:23, 287 Postings

Der AEG Kombiquick – Modellnummer [KMK968000T](#) – verspricht einige Vorteile für die Küche. Er kombiniert Mikrowelle und Backofen. Über einen Steuerknopf soll er sich komfortabel bedienen lassen. Wer möchte, kann ihn auch über eine App bedienen und sich dabei gleich mit Rezepten versorgen lassen.

So weit, so gut. Doch im Prospekt des Herstellers nicht erwähnt sind freilich die potenziellen Risiken des vernetzten Kochens. Da wären etwa Sicherheitslecks und dadurch mögliche Angriffe. Oder fehlerhafte Updates. Mit letzterem Phänomen machten nun Besitzer jenes Kombiquick-Modells in den Niederlanden, in Belgien und Luxemburg Bekanntschaft. Es bescherte ihren Geräten eine veritable Identitätskrise, wie NU.nl berichtet.



Der Mikrowellen/Grill-Kombi-Ofen hält sich seit dem Update für einen Backofen mit Dampffunktion.

Foto: AEG



Wikimedia: Fragen
Wikimedia: The End

Was ist das Internet?

- Was sind Computer-Netze?
- Wie funktioniert Verschlüsselung?
- Was ist Public Key Infrastruktur?
- Was ist die Cloud?
- Was ist ein Hacker Angriff?

Was sind Computer-Netze?

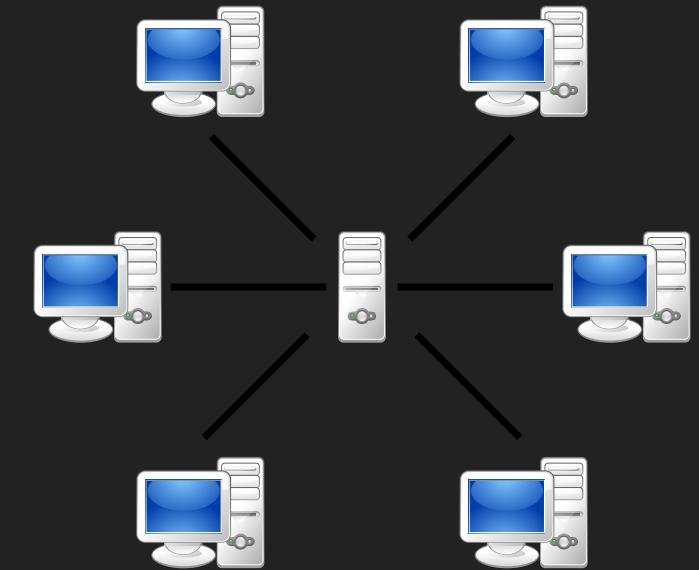
[Wikipedia](#)

Ein [...] Computernetzwerk ist ein Zusammenschluss verschiedener [...] primär selbstständiger elektronischer Systeme [...], der die Kommunikation der einzelnen Systeme untereinander ermöglicht. Ziel ist hierbei z. B. die gemeinsame Nutzung von Ressourcen wie Netzwerkdruckern, Servern, Dateien und Datenbanken. [...] Besondere Bedeutung hat heute auch die direkte Kommunikation zwischen den Netzwerknutzern (Chat, VoIP-Telefonie etc.).

Client-Server Architektur

[Wikipedia](#)

Das Client-Server-Modell [...] beschreibt eine Möglichkeit, Aufgaben und Dienstleistungen innerhalb eines Netzwerkes zu verteilen. [...] Der Client kann auf Wunsch einen Dienst vom Server anfordern [...]. Der Server [...] beantwortet die Anforderung [...]; üblicherweise kann ein Server gleichzeitig für mehrere Clients arbeiten.



Grafik: Wikipedia (Mauro Bieg)

Internet

[Wikipedia](#)

Das Internet [...] ist ein weltweiter Verbund von Rechnernetzwerken [...]. Es ermöglicht die Nutzung von Internetdiensten wie WWW, E-Mail, [...] Der Datenaustausch zwischen den über das Internet verbundenen Rechnern erfolgt über die technisch normierten Internetprotokolle.

HTML

Wikipedia

Die Hypertext Markup Language [...] ist eine textbasierte Auszeichnungssprache zur Strukturierung elektronischer Dokumente [...]. HTML-Dokumente sind die Grundlage des World Wide Web und werden von Webbrowsern dargestellt.

- statische Beschreibung der Inhalte
- wird vom Web-Server ausgeliefert und vom Browser dargestellt

Grafik: Wikipedia

```
<!DOCTYPE html>
<html>
<!-- created 2010-01-01 -->
<head>
  <title>sample</title>
</head>
<body>
  <p>Voluptatem accusantium  
totam rem aperiam.</p>
</body>
</html>
```

HTML

JavaScript

Wikipedia

JavaScript [...] ist eine Skriptsprache, die ursprünglich [...] für dynamisches HTML in Webbrowsern entwickelt wurde, um Benutzerinteraktionen auszuwerten, Inhalte zu verändern, nachzuladen oder zu generieren und so die Möglichkeiten von HTML zu erweitern.

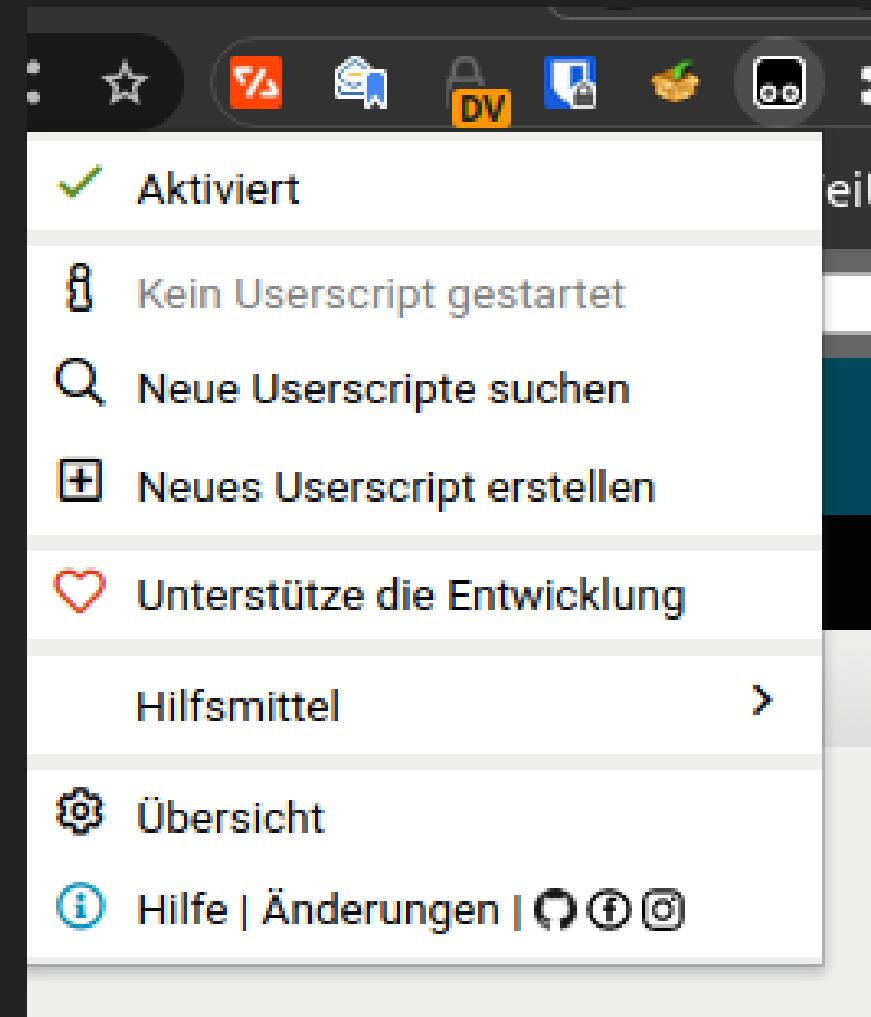
- dynamische Inhalte
- Programm das vom Server geladen und vom Browser ausgeführt wird

```
// Beispiel JavaScript
function halloWelt() {
    alert('Hello World');
}
window.onload = halloWelt;
```

Grafik: Wikipedia

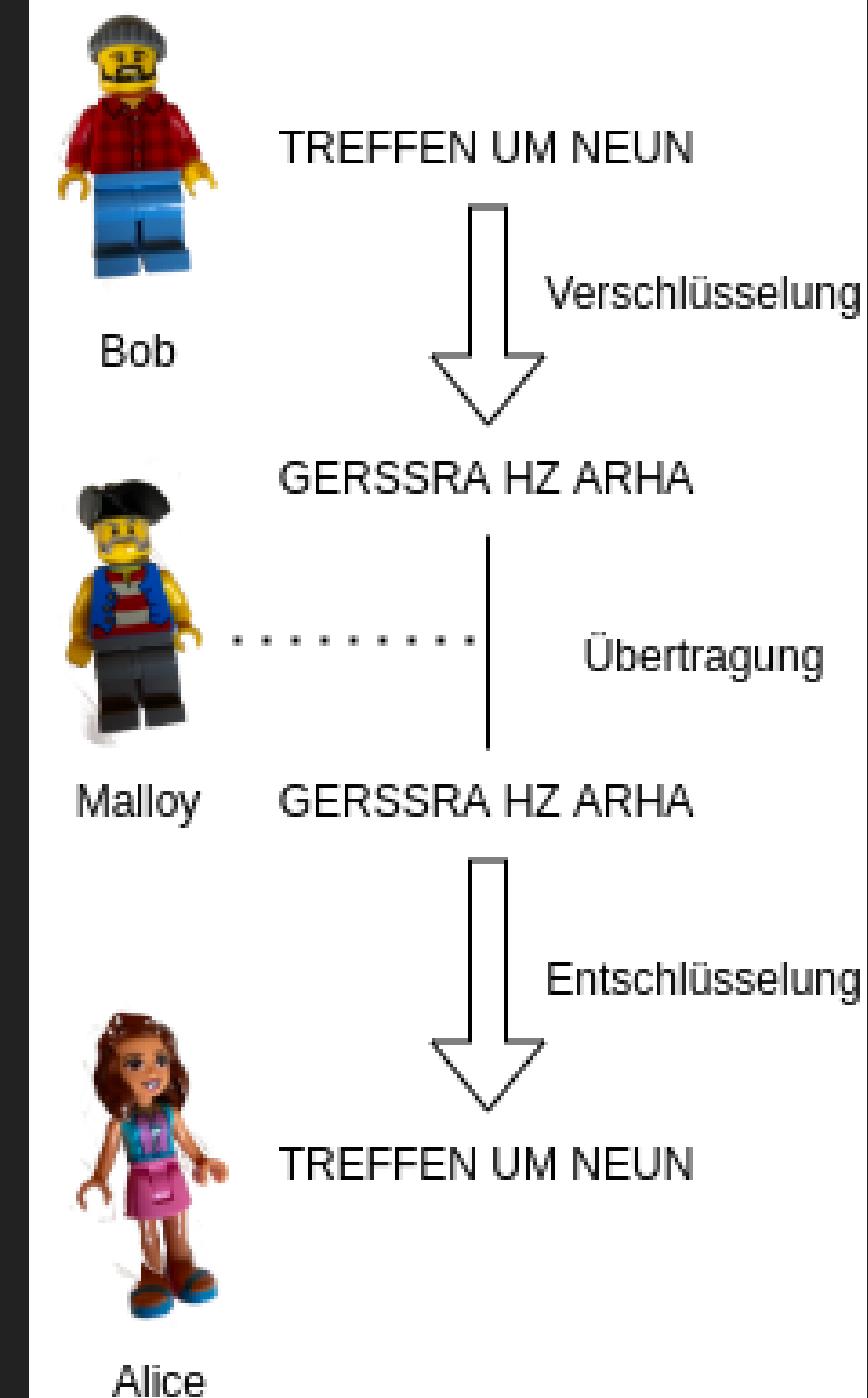
Exkurs: MonkeyScript

- JavaScript wird vom Browser ausgeführt
- Benutzer kann JavaScript manipulieren
- Änderung ist nur "lokal" (auf dem eigenen Rechner) sichtbar
- Tampermonkey/Greasemonkey erlaubt eigene Skripts "hinzuzufügen"



Wie funktioniert Verschlüsselung?

- Bob will Alice eine Nachricht schicken
- Malloy will die Nachricht lesen
- Bob und Alice haben ein gemeinsames Passwort
- Algorithmus ist öffentlich, Passwort ist geheim



Transport Layer Security (TLS/SSL)

[Wikipedia](#)

Transport Layer Security [...], auch bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

- Daten vom Client zum Server werden verschlüsselt
- Metadaten (wer kommuniziert wann mit wem) sind nicht verschlüsselt

Exkurs: eMail

- Inhalte sind unverschlüsselt
 - S/MIME / PGP/MIME sind Erweiterungen um den Inhalt zu verschlüsseln
- der Absender kann leicht "gefälscht" werden
- SMTP: senden von eMails
- POP3/IMAP: empfangen von eMails

```
1: > 220 mail.example.com SMTP Foo Mailserver
2: < HELO mail.example.org
3: > 250 Ok
4: < MAIL FROM: hans.muster@example.org
5: > 250 Ok
6: < RCPT TO: foo@example.com
7: > 250 Ok
8: < DATA
9: > 354 End data with .
10: < From: hans.muster@example.org
11: < To: foo@example.com
12: < Subject: Testmail
13: <
14: < Testmail
15: < .
16: > 250 Ok
17: < QUIT
18: > 221 Bye
```

Grafik: Elektronik Kompendium

Ende-zu-Ende-Verschlüsselung

- ohne Ende-zu-Ende-Verschlüsselung:
 - TLS schützt nur auf dem Transportweg
 - jeder Server kann die Inhalte lesen/manipulieren
- Ende-zu-Ende-Verschlüsselung:
 - Inhalte sind geschützt
 - Metadaten (wer kommuniziert wann mit wem) ist "öffentlich"

Exkurs: Metadaten

Bundesamt für Sicherheit in der Informationstechnik (BSI):

Nachrichten, die über Messenger verschickt werden, bestehen aus dem Text der Nachricht [...] und sogenannten Metadaten. Zu den Metadaten zählen die Kennung des Absenders, häufig in der Form der Telefonnummer, die Kennung des Adressaten, das Datum und die Uhrzeit. [...] Solche Daten dienen nicht nur der korrekten Zuleitung der Nachricht, sondern können auch zur Analyse von Vorlieben und ähnlichem genutzt werden. Auf diese Weise lassen sich Profile erstellen, die für personalisierte Werbung genutzt werden können.

- SpiegelMining zeigt was mit Metadaten möglich ist

Was ist Public Key Infrastruktur?

Wikipedia:

Mit Public-Key-Infrastruktur [...] bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

- basiert auf **asymmetrischer Verschlüsselung**
- Anwendungen: **HTTPS, Corona Impfzertifikate**

Zertifikats-Viewer: *.google.com

Allgemein Details

Ausgestellt für

Allgemeiner Name (CN)	*.google.com
Organisation (O)	<Gehört nicht zum Zertifikat>
Organisationseinheit (OU)	<Gehört nicht zum Zertifikat>

Ausgestellt von

Allgemeiner Name (CN)	GTS CA 1C3
Organisation (O)	Google Trust Services LLC
Organisationseinheit (OU)	<Gehört nicht zum Zertifikat>

Gültigkeitsdauer

Ausgestellt am	Montag, 15. August 2022 um 10:17:55
Gültig bis	Montag, 7. November 2022 um 09:17:54

Fingerabdrücke

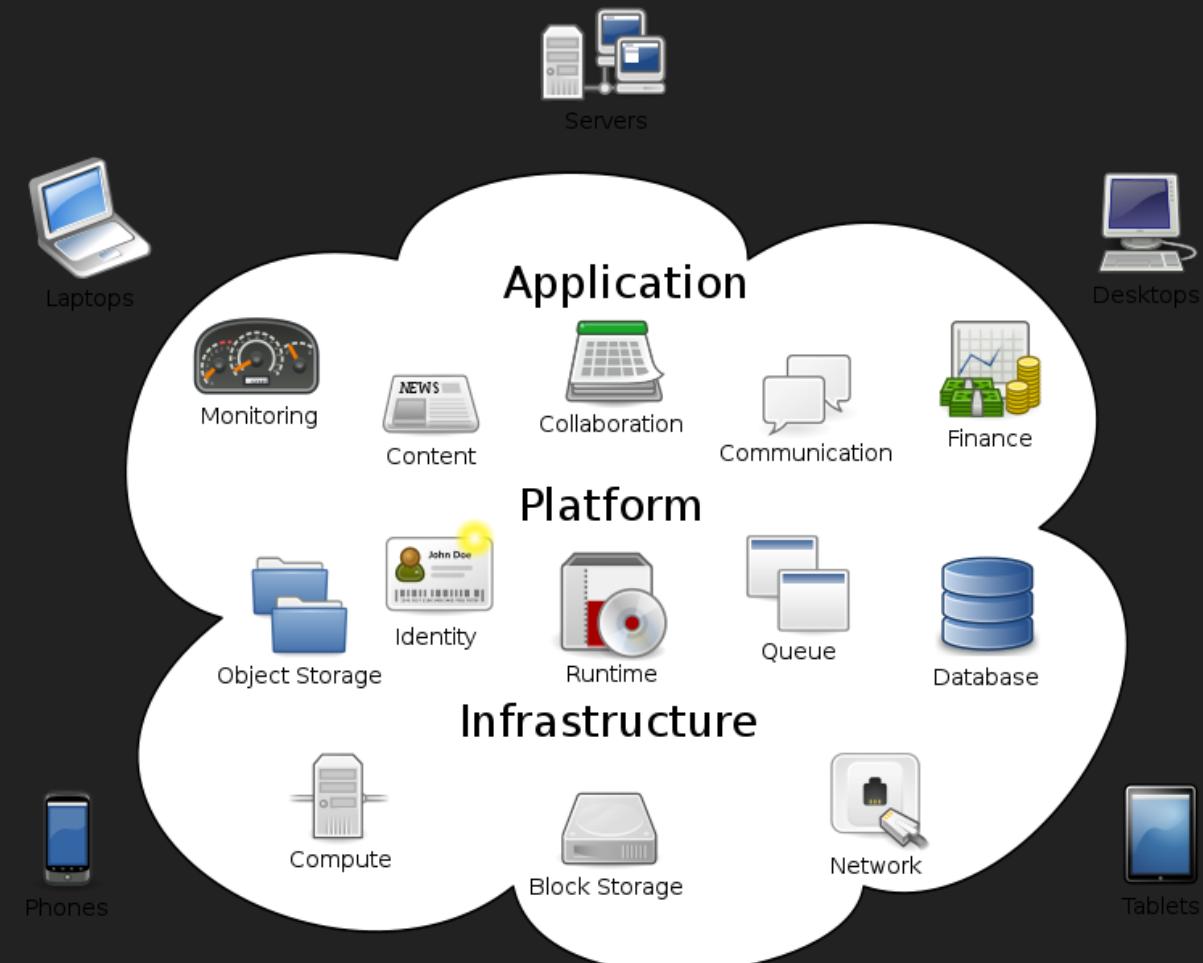
SHA-256-Fingerabdruck	99 18 E3 F0 D1 50 A4 A9 A7 EB 3F 98 79 D7 69 C0 FB 70 7E 88 7E F7 3B 35 CB 77 4A 2C FE 31 1C A1
SHA-1-Fingerabdruck	01 02 2A 5D 8D C6 A1 46 03 58 6F 6E 2A 54 0F AC 43 A7 38 6C

Was ist die Cloud?

Wikipedia:

Cloud Computing [...] beschreibt ein Modell, das bei Bedarf [...] zeitnah und mit wenig Aufwand geteilte Computerressourcen als Dienstleistung [...] bereitstellt und nach Nutzung abrechnet.

- ohne Verschlüsselung hat der Cloud-Anbieter Datenzugriff



Grafik: Wikipedia

Was ist ein Hacker-Angriff?

Wikipedia: Black-Hat

Black-Hats [...] handeln mit krimineller Energie [...] und beabsichtigen [...] das Zielsystem zu beschädigen oder Daten zu stehlen[...].

- kriminelle oder staatliche motivierte Manipulation von fremden Computern
- Angriffswege:
 - Benutzer ([Phishing](#), [Social Engineering](#))
 - schlechte Konfiguration (Standard-Passwörter)
 - Softwarefehler ([CVE](#))

Wie funktioniert ein Hacker-Angriff?

- Zugriff erlangen über einen Angriffs weg
- Zugriff sicher - "unsichtbar" für das Opfer
- Zugriff ausweiten - andere Geräte im Netzwerk
- Profit erzielen:
 - Daten stehlen und verkaufen (Kreditkarten, Firmengeheimnisse, ...)
 - Ransomware
- Selten: **DoS** ("digitaler Sitzstreik") - Dienst wird durch Überlastung für Benutzer nicht mehr erreichbar

Ransomware

- Erpressungssoftware
- Daten werden verschlüsselt
- Unternehmen: Daten werden gestohlen

Grafik: Wikipedia



Ist mein Auto ein Computer? Ja!

- ECU: "electronic control unit" - eingebettetes System
- ECUs bilden ein Computer-Netzwerk - Kommunikation über CAN/LIN/FlexRay/Ethernet
- bisherige Fahrzeuge beinhalten ein Netzwerk von bis zu mehr als hundert ECUs
- moderne Fahrzeuge setzen auf mehreren HPCs (High Performance Computer) mit virtuellen Maschinen (Linux, QNX) die mit Gigabit-Ethernet Netzwerken kommunizieren



Wikimedia: Fragen
Wikimedia: The End