max planck institut
informatik

Ideen und Konzepte der Informatik

Eine Vorlesung für Hörer aller Fakultäten

Einführung

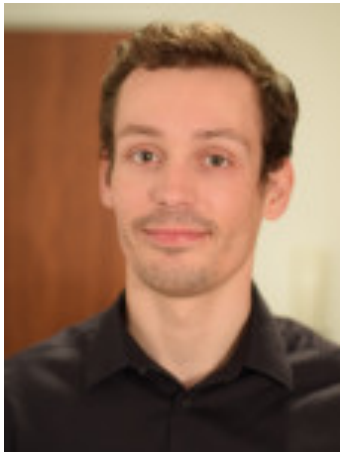
Privatheit & Sicherheit

Antonios Antoniadis

Die Dozenten

Kurt Mehlhorn

- Studium: Mathematik, Physik, Informatik
- Direktor AG1, MPII
- Prof. an der UdS
- Vielzahl renommierter Forschungspreise



Antonios Antoniadis

- Studium: Angewandte Mathematik, Informatik
- PostDoc am MPII und an der UdS
- DFG-Forschungsprojekt: Algorithmen für Energieeffiziente Berechnungen

André Nusser

- Tutor
- Promoviert in der Gruppe Algorithmen & Komplexität

Organisation

- keine Vorkenntnisse erforderlich, nur Neugier
- Vorlesung: montags, 16 – 18 Uhr, E1.4, Raum 024
- Übungen: montags und dienstags, 14 – 16 Uhr, und freitags 10 – 12 Uhr.
- Schein (5 Leistungspunkte)
  - erfolgreiche Teilnahme an Übungen (45% der Punkte)
  - Klausur: Montag, 5.2, 16:15 – 18:15 Uhr
  - Gesamtnote ist Klausurnote
  - Nachklausur zu Beginn des Sommersemesters
  - Informatiker können keinen Schein erwerben

Ziele

- Grundbegriffe der Informatik vermitteln: Was ist ein Computer? Ein Algorithmus? Sind alle Computer gleich? Können Computer alles? Mit welchem Aufwand? Intelligenz?
- Wichtige Informatiksysteme: Suchmaschinen, WWW, Navigationssysteme.
- Grundlage für fundierte Diskussionen über die enormen gesellschaftlichen Konsequenzen der Informatik (positiv und negativ).

Ziele der Vorlesung

- **Grundbegriffe der Informatik:**
  - Was ist ein Computer (Hardware, Software)? Sind alle Computer gleich? Was ist ein Algorithmus? Können Computer alles? Mit welchem Aufwand? Lernen? Intelligenz?
- **Wichtige Informatiksysteme:**
  - Suchmaschinen, Datenbanksysteme, WWW, Electronic Banking, Navigationsysteme, Autonome Maschinen, Lernende Systeme
- **Algorithmisches Denken**
- **Grundlage für Diskussionen über die enormen gesellschaftlichen Konsequenzen der Informatik**

Informatik verändert die Welt

Internet, Suchmaschinen, Mobiltelefonie, Electronic Banking, Einkaufen im Internet, Entzifferung des menschlichen Genoms, Klimavorhersage, Navigationssysteme, soziale Netzwerke, Wikipedia, Digitale Kameras, Roboter, Soziale Netzwerke, Wissenschaft (Rechts-, Bio-, Wirtschafts-, …, Medizininformatik), Simulation.

Viele dieser Errungenschaften sind recht neu; nicht mehr wegdenkbar; wirtschaftlich bedeutend; verändern Verhalten Einzelner und der Gesellschaft

KM benutzt

- E-Mail seit 1985
- Textverarbeitung seit 1986
- Vorträge mit dem Rechner seit 1992
- Hat eine Homepage seit 1996
- Rechner auch für private Zwecke (Electronic Banking, Reisen planen, Informationssuche, Navi, Digitale Kamera, email, Whatsapp, Online Einkaufen) **nach 2000**

Ein Rechnerraum (1910)

Auch die Bedeutung von Worten ändert sich.

Fließband

Warum diese Vorlesung?

- Jeder sollte Informatikwissen haben.
- Um die neue Welt mit ihren positiven und negativen Konsequenzen besser zu verstehen.
- Dazu genügt nicht: Umgang mit Windows, Word, Browser, Google, Facebook, ….
- Konzepte und nicht nur Errungenschaften.

Themen der Vorlesung

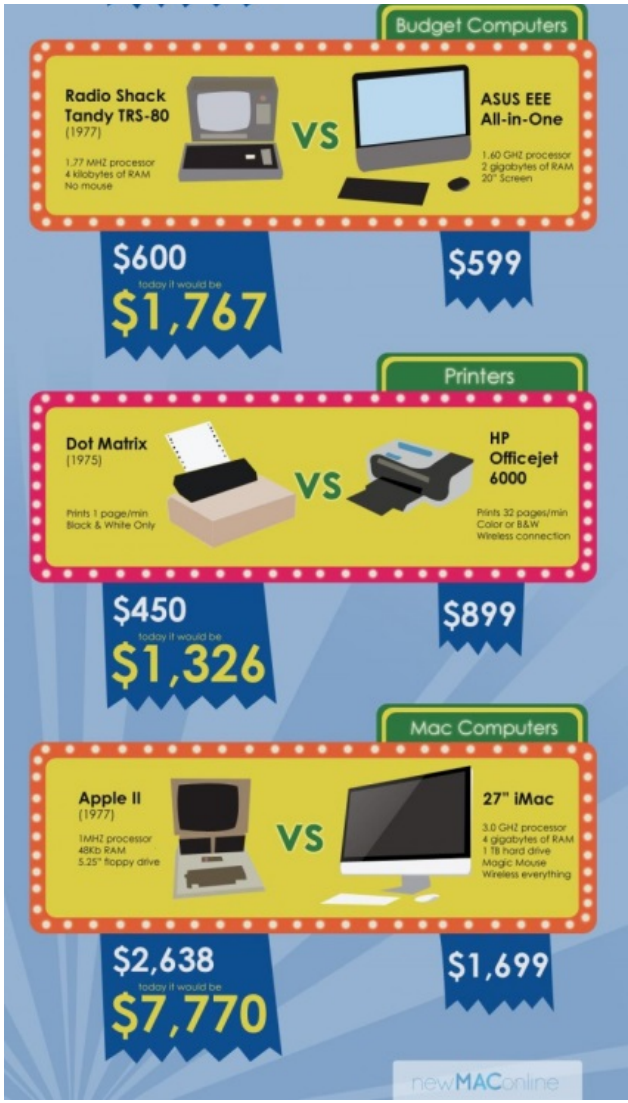
- Was ist ein Computer?
- Was ist ein Programm?
- Moderne Computer
- Können Computer alles?
- Das Internet
- Kürzeste Wege und Navis
- Suchen und Sortieren
- Bitcoins
- Suchmaschinen
- Kryptographie und Sicherheit
- Maschinelles Lernen
- Komplexität, Entscheidbarkeit, P und NP
- Rechnen und Zufall
- Optimierung

Moore's „Law“ (1965)

- Anzahl der Transistoren pro Chip verdoppelt sich alle zwei Jahre.
- 1965 → 2015 = 50 Jahre, 2^{25} = 32 Mio
- ähnlich: Prozessorgeschwindigkeit, Speicherkapazität, Rechnerleistung pro Watt oder pro Euro Kaufpreis, Bandbreite von Netzwerken
- Leistung der Physik und Ingenieurwissenschaften.

Moore's „Law“ (1965)

- Anzahl der Transistoren pro Chip verdoppelt sich alle zwei Jahre.
- 1965 → 2015 = 50 Jahre, 2^{25} = 32 Mio
- ähnlich: Prozessorgeschwindigkeit, Speicherkapazität, Rechnerleistung pro Watt oder pro Euro Kaufpreis, Bandbreite von Netzwerken
- Leistung der Physik und Ingenieurwissenschaften.



Große Trends

- Automatisierung und Optimierung
- Kommunikation
- Datenanalyse
- Autonome Systeme
- Informatik schafft Geräte zur Intelligenzverstärkung, davor nur Kraftverstärkung

Automatisierung: Post

- Werfe Brief in den Postkasten
- Kasten → Zentrale
- Sortieren
- Transport nächste Zentrale
- Sortieren
- Brief austragen

- Ein Click auf Wegschicken
- INFORMATIK
- Brief im Posteingang

Zustellung überall

Aber: Postgeheimnis

Automatisierung: Industrie

Ford Model T (1912)

You can have any color as long as it is black

BMW 2016

Man kann zwischen Millionen von Varianten wählen

Entwurfsprozess stark rechnergestützt

Gesamtsteuerung einer Fabrikation einschl. Zulieferer

Losgröße eins ist das Ziel.

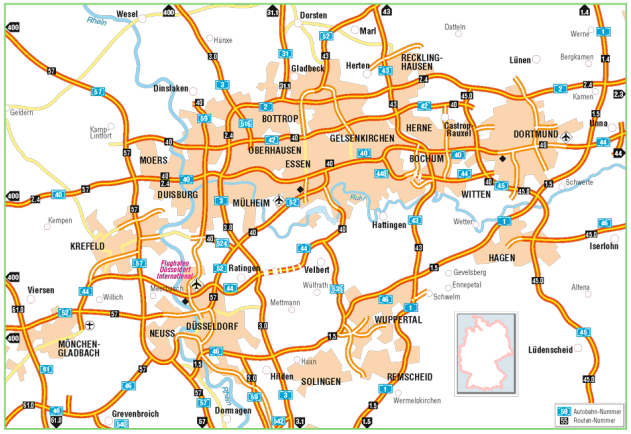
Optimierung: Navigation

Bis etwa 2005

Studium von Karten

Häufiges Verfahren und Verlaufen

Suboptimale Lösungen



heute

Schnellste Wege mit einem Mausklick

Auto, Fußgänger, Bahn, Bus, Flugzeug.

Integration der verschiedenen Transportarten

Nebenbedingungen

Automatisierung: Reise

- Katalog studieren
- Ins Reisebüro gehen und Wünsche formulieren
- Reisebüro kontaktiert Hotels, Fluggesellschaft
- Mehrere Stunden oder Tage warten
- Im Internet informieren (mit Videos, Empfehlungen)
- Online buchen

Kommunikation

- E-Mail
- Soziale Netzwerke
  - Facebook, Xing, ResearchGate
- Mobiltelefonie und Skype
- Internetbanking, sichere Kommunikation

- Geschwindigkeit und Verfügbarkeit ↑
- Kosten ↓

Datenanalyse

- Wer dieses Buch gekauft hat, hat auch …
- Entzifferung des menschlichen Genoms
  - Länge, 6 Milliarden Buchstaben
- Personalisierte Werbung, Personalisierte Nachrichten
- Personalisierte Medizin
- Usw.

Neue Dienste

- Airbnb, Uber
- Carsharing
- MOOCS (Massive Online Courses)
- Einkaufen im Internet
- Maschinelle Übersetzung
- Autonome Maschinen

Maschinelle Übersetzung (Google Translate)

Mehlhorn graduated in 1971 from the Technical University of Munich, where he studied computer science and mathematics, and earned his Ph.D. in 1974 from Cornell University under the supervision of Robert Constable.

Mehlhorn studierte 1971 an der Technischen Universität München, wo er studierte Informatik und Mathematik und promovierte im Jahr 1974 von der Cornell University unter der Leitung von Robert Constable.

Autonome Maschinen

Mähroboter

Selbstfahrendes Auto

Negative Auswirkungen

- Wegfallende oder stark reduzierte Berufe: Schriftsetzer, Reisebüro, Bandarbeit, Büroarbeit, Taxifahrer, …
- Was weiß Google über Sie? Geschlecht, Altersgruppe, Krankheiten.
- Wer weiß mehr über Sie als Google?
- Personalisierte Nachrichten: Algorithmen bestimmen, welche Information Sie bekommen.
- Winner takes it all (Google vs. Yahoo, Facebook vs. ….)
- Das Internet vergisst nichts.
- Neue Formen von Sucht.

Zusammenfassung

- Informatik hat die Welt revolutioniert und wird sie weiter verändern
- Große Chancen für eine bessere Welt, aber auch Gefahren für Privatheit, Sicherheit, …
- Jeder sollte Informatikwissen haben.

Teil II

Privatheit und Sicherheit

Praktische Tipps

Überblick

- Sicherheit:
  - Absperren von Geräten
  - Back-Ups (Datensicherung)
  - Passwörter
  - Soziale Attacken, Phishing,
- Privatheit
- Man sollte nicht paranoid bezüglich Sicherheit und Privatheit sein.

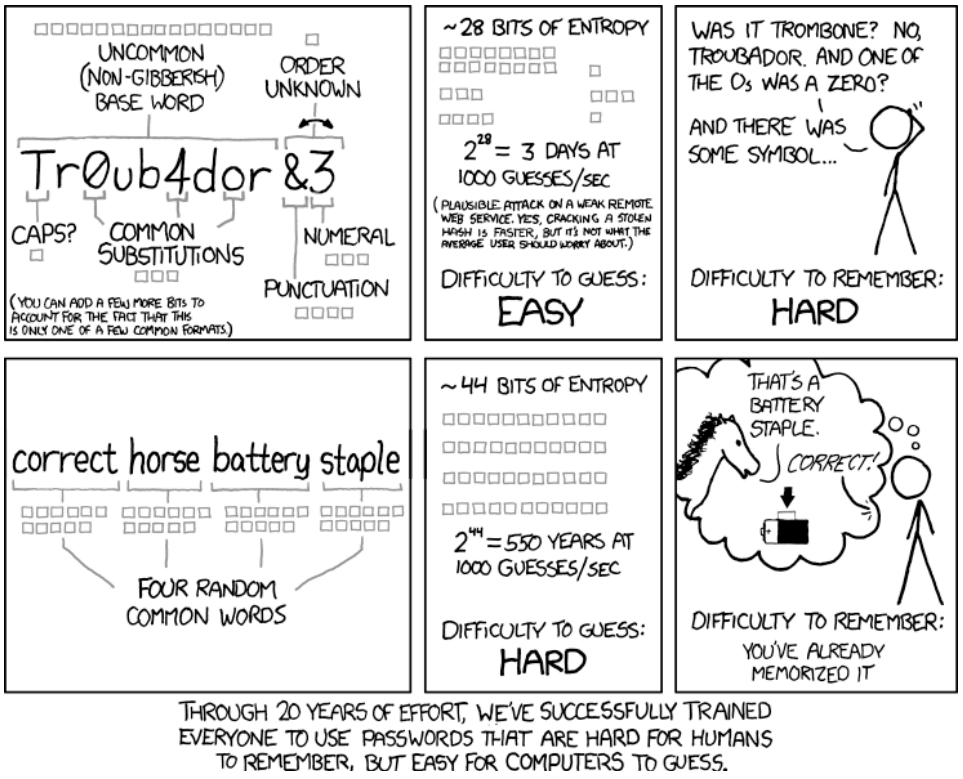
Sicherheit

Eine Kette ist nur so stark wie ihr schwächstes Glied.

Passwörter I

- Für meine Anwendungen (Banken, Internetstores, Zeitungen, E-Mails, Benutzerkonto am MPII ….) benutze ich Passwörter unterschiedlicher Qualität.
- Für wichtige Dienste (hoher Schaden) jeweils ein eigenes Passwort
- Für unwichtige Dienste (kleiner Schaden) einige wenige Passwörter.
- Fast alle Passwörter sind 8 Zeichen oder länger. Wichtige Passwörter sind 12 und mehr Zeichen.

Passwörter II



Lieber Längere Passwörter als kurze mit mehr “Sonderzeichen”

Wichtig: Passwort sollte nicht 1 zu 1 im Internet (z.B. Wörterbuch, Literatur usw.) zu finden sein.

Passwörter III

- Ich benutze einen Passwortsafe (Keepassx, Keychain), den ich zwischen meinen verschiedenen Geräten automatisch synchronisiere.
- Dafür benutze ich ein langes Passwort (14 Zeichen).
- Den Passwortsafe in meinem Browser benutze ich nur für unwichtige Passwörter.

Absperren von Geräten

- Meine Geräte werden gesperrt, wenn ich sie 60 Sekunden nicht benutze
- Iphone, Ipad: 4stelliger Code, 3mal falscher Code führt zum Löschen aller Inhalte
- Notebook: Passwort mit 12 Zeichen
- WLAN zu Hause: Passwort mit 12 Zeichen

Datensicherung (Back-Up)

- Machen sie regelmäßig eine Datensicherung auf ein Medium, das getrennt von ihrem Rechner ist
- KM auf der Arbeit: automatisch, wenn immer er mehrere Stunden im Büro ist
- KM zu Hause: wöchentlich oder öfter bei Bedarf auf Festplatte, die er nur dazu mit dem Rechner verbindet.
- Telefon und Ipad regelmäßig auf Rechner zu Hause

Weitere Maßnahmen

- HTTPS Everywhere
- Vorsicht beim Öffnen von Attachments und Verfolgen von Links. Besondere Vorsicht, wenn Absender oder Webseite unbekannt.
- Aktuelle Version des Betriebssystems und aller Programme (automatische Updates).
- Virenscanner – Vor- aber auch Nachteile
- Nicht mit Administratorrechten arbeiten.
- Uni Bielefeld: 10 goldene Regeln für Computersicherheit.

Phishing


Stadtsparkasse München
ır geehrter Kunde,
gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind
genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München
:hzuführen.
Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues
ensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die
tokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu
:ellt.
lgedessen bitten wir Sie, eine spezielle Form der zusätzlichen Autorisation auszufüllen.
FORM AUSFÜLLEN
se Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.
ıke für Ihre Zusammenarbeitarbeit,
ninistration der Stadtsparkasse München
NICHT WIRKLICH SPARKASSE!
© 2005 Stadtsparkasse München

Privatheit

Es gibt wenig umsonst im Internet. In der Regel zahlen wir mit Daten, die

- eine gezieltere Werbung erlauben oder
- für Angriffe benutzt werden können

oder direkt mit höherer Verwundbarkeit.

Das Internet vergisst nicht. Was wir heute lustig finden, finden wir in 10 Jahren vielleicht peinlich.

Dienste

- Ich benutze Browser, Google, WhatsApp, Threema, Signal, email (immer weniger gmail), Dropbox.
- Browser: maximale Sicherheits- und Privatheitseinstellungen.
- Browsererweiterungen Adblock, HTTPS Everywhere, Privacy Badger (protection against trackers), Google Analytics Opt-Out, NoScript.
- Google Privatsphärecheck: habe die Rechte von Google zur Auswertung meines Browserverhaltens weitmöglichst eingeschränkt.

Email

- KM signiert seine emails (Elektronische Unterschrift)
- Manche emails verschlüsselt er (wenn der Empfänger es so eingerichtet hat)