Script **generated by TTT**

Title: Einf_HF (16.07.2012)

Date: Mon Jul 16 14:18:18 CEST 2012

Duration: 91:51 min

Pages: 62

IP-Adresskonzept

Teil des TCP/IP-Referenzmodells ist die Festlegung der Adressierung von Rechnern im Netz. Dazu erhält jedes Computersystem eine eindeutige "Rufnummer", seine IP-Adresse. Eine IP-Adresse besteht aus vier Byte. Diese werden üblicherweise dezimal durch Punkte getrennt geschrieben, z.B. 131.159.24.30

Die weltweit eindeutige Vergabe von IP-Adressen übernehmen die NICs (Network Information Center). In Deutschland ist das beispielsweise das DENIC .

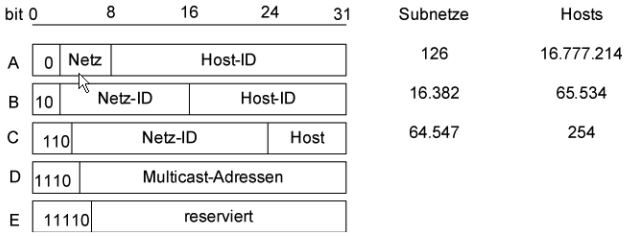
Adressklassen

Neben den IP-Adressen können Computersysteme noch einen oder mehrere einfach zu merkende Namen bekommen, wie z.B. www.in.tum.de. Die möglichen letzten Silben (top level domain) sind global festgelegt, die zweitletzte Silbe wird von jeweils zuständigen Stellen vergeben (für die .de-Domäne beispielsweise DE-NIC)

Durch den Boom des Internet werden die Adressen bereits knapp; deshalb Erweiterung der IP-Adressen auf 128 Bit (IPv6 Adresskonzept).

Generated by Targeteam

IP-Adressen werden in Blöcke zusammengefasst um die Netzverwaltung zu erleichtern. Die Adresse besteht dazu aus Netz-ID und Host-ID. Nur die Netz-IDs werden zentral vom Network Information Center vergeben. Die Klasse gibt an, wie groß der Byte-Anteil der Netz-ID ist.



	Subnetze	Hosts
A	126	16.777.214
B	16.382	65.534
C	64.547	254

Klasse A: Adressbereich 1.0.0.0 - 127.255.255.255

Klasse B: Adressbereich 128.0.0.0 - 191.255.255.255

Klasse C: Adressbereich 192.0.0.0 - 223.255.255.255

Klasse D: Adressbereich 224.0.0.0 - 239.255.255.255 (verwendet durch Videokonferenzsysteme)

Klasse E: Adressbereich 240.0.0.0 - 247.255.255.255

Generated by Targeteam

IP-Adresskonzept

Teil des TCP/IP-Referenzmodells ist die Festlegung der Adressierung von Rechnern im Netz. Dazu erhält jedes Computersystem eine eindeutige "Rufnummer", seine IP-Adresse. Eine IP-Adresse besteht aus vier Byte. Diese werden üblicherweise dezimal durch Punkte getrennt geschrieben, z.B. 131.159.24.30

Die weltweit eindeutige Vergabe von IP-Adressen übernehmen die NICs (Network Information Center). In Deutschland ist das beispielsweise das DENIC .

Adressklassen

Neben den IP-Adressen können Computersysteme noch einen oder mehrere einfach zu merkende Namen bekommen, wie z.B. www.in.tum.de. Die möglichen letzten Silben (top level domain) sind global festgelegt, die zweitletzte Silbe wird von jeweils zuständigen Stellen vergeben (für die .de-Domäne beispielsweise DE-NIC)

Durch den Boom des Internet werden die Adressen bereits knapp; deshalb Erweiterung der IP-Adressen auf 128 Bit (IPv6 Adresskonzept).

Generated by Targeteam

- Verteilte Informationsverarbeitung nutzt die Verbindung mehrerer Rechner durch Rechnernetze zum Aufbau komplexer Systeme, die mehr als einen Rechner einbeziehen. Hier gehen wir näher auf Verteilte Anwendungen im Allgemeinen und auf das momentan in diesem Zusammenhang wichtigste Teilgebiet E-Commerce ein. Weiterhin werden Sicherheitsfragen bei Verteilten Anwendungen behandelt.
- Fragestellungen des Abschnitts:
  - Was versteht man unter dem Client/Server-Modell?
  - Was versteht man unter Verschlüsselung? Welche grundlegenden Verfahren gibt es?
  - Was versteht man unter digitalen Signaturen?

Verteilte Anwendungen

Sicherheit in verteilten Systemen

Aufteilung einer Anwendung in Komponenten (einzelne Programme auf verschiedenen Rechnern), die miteinander kommunizieren um einen Dienst zu erbringen.

Entwicklung hin zu verteilten Anwendungen

Verteilte Systeme

Client-Server-Modell

Beispiel-Services

World Wide Web

Verteilte Anwendungen

Aufteilung einer Anwendung in Komponenten (einzelne Programme auf verschiedenen Rechnern), die miteinander kommunizieren um einen Dienst zu erbringen.

Entwicklung hin zu verteilten Anwendungen

Verteilte Systeme

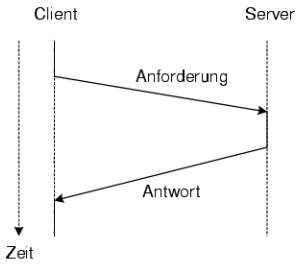
Client-Server-Modell

Beispiel-Services

World Wide Web

Möglichkeit zur Strukturierung von (verteilten) Anwendungen: ***Server*** stellen Dienste zur Verfügung, die von (den Servern) vorher unbekannten ***Clients*** in Anspruch genommen werden können.

Client und Server



Client ruft Operation eines Servers auf, erhält ggf. Ergebnis zurück. Während Operation wird Ablauf des Client meist unterbrochen.

Definition: Client

Anwendungsteil, der auf Anforderung einen Dienst von einem Server erhält.

Clients sind meist a-priori beim Server nicht bekannt.

Definition: Server

Subsystem, das bestimmten Dienst für a-priori unbekannte Clients zur Verfügung stellt.

Client und Server kommunizieren über Nachrichten.

Antwort bestätigt Empfang der Anforderung durch den Server.

Beispiel-Services

Datei-Service

Entfernte, zentralisierte Datenspeicherung für Arbeitsplatzrechner.

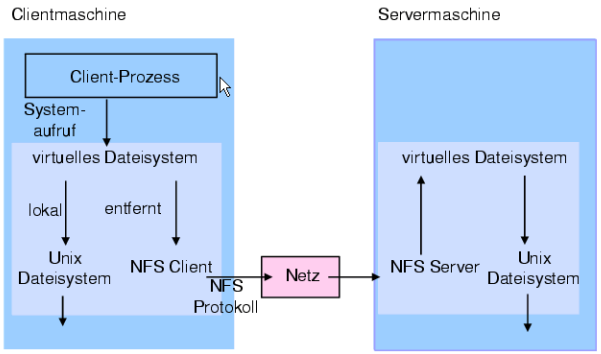
Beispiel NFS (Network File System)

Namens-Service

Entfernte, zentralisierte Namensverwaltung für Objekte (Dateien, andere Server, Services, Drucker, Benutzer etc.).

Zeit-Service

Synchronisierte Systemzeit für Rechner.



Datei-Service

Entfernte, zentralisierte Datenspeicherung für Arbeitsplatzrechner.

Beispiel NFS (Network File System)

Namens-Service

Entfernte, zentralisierte Namensverwaltung für Objekte (Dateien, andere Server, Services, Drucker, Benutzer etc.).

Zeit-Service

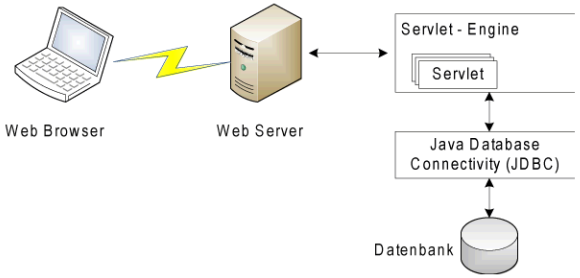
Synchronisierte Systemzeit für Rechner.

Generated by Targeteam

Organisiert nach Client/Server Architektur.

- Zieladresse wird mit Hilfe einer URL angegeben
  - Beispiel: http://www11.in.tum.de/lehre/vorlesungen/
    - http:// gibt das Kommunikationsprotokoll für den Zugriff auf Web-Seiten an.
    - www11.in.tum.de gibt den Web-Server an.
    - lehre/vorlesungen/ gibt ein Verzeichnis/Dokument innerhalb des Web-Servers an.
    - Standardport des Web-Servers: 80.
  - Weitere Kommunikationsprotokolle
    - https:// Kommunikationsprotokoll für den gesicherten Zugriff auf Web-Seiten.
    - file:// Zugriff auf Dateien am lokalen Rechner.
    - ftp:// Zugriff auf Dateien an einem entfernten Rechner; Nutzung des Filetransfer Dienstes.
    - mailto: verschicken von Emails an die angegebene Adresse.
  - Methoden des http Protokolls
    - GET: anfordern einer Ressource (z.B. eine Web-Seite), die mittels einer URL spezifiziert ist.
    - PUT: dient dazu eine Ressource (z. B. eine Web-Seite) unter Angabe der Ziel-URL auf einen Webserver hochzuladen.

Mit Hilfe von Informationen aus Datenbanken können Inhalte von Web-Seiten dynamisch gestaltet werden; dazu Abruf der DB-Information über Servlets und spezielle Schnittstellen, z.B. Java DB Connectivity (JDBC).



Anwendungen von Rechnernetzen

- Verteilte Informationsverarbeitung nutzt die Verbindung mehrerer Rechner durch Rechnernetze zum Aufbau komplexer Systeme, die mehr als einen Rechner einbeziehen. Hier gehen wir näher auf Verteilte Anwendungen im Allgemeinen und auf das momentan in diesem Zusammenhang wichtigste Teilgebiet E-Commerce ein. Weiterhin werden Sicherheitsfragen bei Verteilten Anwendungen behandelt.
- Fragestellungen des Abschnitts:
  - Was versteht man unter dem Client/Server-Modell?
  - Was versteht man unter Verschlüsselung? Welche grundlegenden Verfahren gibt es?
  - Was versteht man unter digitalen Signaturen?

Verteilte Anwendungen

Sicherheit in verteilten Systemen

Sicherheit in verteilten Systemen

Ein wichtiger Aspekt eines Rechnersystems besteht darin, dass Daten nicht von Unbefugten abgefragt werden können. Bei nicht-vernetzten Systemen läßt sich dies durch eine Sicherung des physikalischen Zugangs zu den Rechnern und einfache Passwortsysteme garantieren. Bei verteilten Systemen werden zusätzliche Dienste benötigt.

Sicherheitsanforderungen

Verschlüsselung

Identitätsprüfung

Sicherheitsanforderungen

Garantierung der Identität eines Absenders (Identitätsprüfung, Authentifizierung).

Verhinderung von Mithören (Verschlüsselung).

Sicherstellung der Integrität (Unverfälschtheit) von Nachrichten (Hash-Werte).

Verhinderung des Wiedereinspielens von Nachrichten (Integritätssicherung und Zeitstempel).

Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.

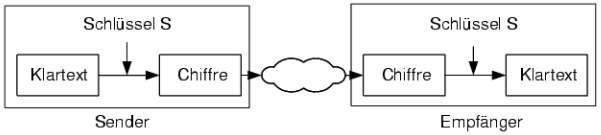
Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).

Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.

Symmetrische Verschlüsselung

Asymmetrische Kryptosysteme

Beide Partner (Sender und Empfänger) kennen einen geheimen Schlüssel, der zum Ver- und zum Entschlüsseln verwendet wird. Eine Kenntnis des Schlüssels erlaubt Zugriff auf die Daten.



Austausch des geheimen Schlüssels über einen anderen, sicheren Kommunikationskanal (z.B. persönlich, Brief)

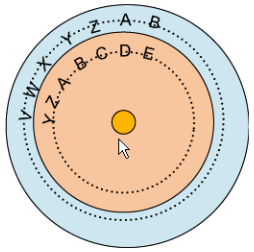
Für jede mögliche Verbindung wird ein eigener Schlüssel benötigt (Falls derselbe Schlüssel für Nachrichten an B und C benutzt wird, könnte C Nachrichten an B lesen).

Beispiele: DES, Tripple DES, IDEA

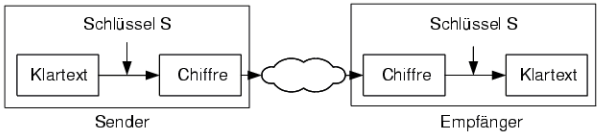
Animation Symmetrische Verschlüsselung

Erweiterte Caesar-Chiffre

- Verschlüsselungsanweisung: Ersetze jeden Buchstaben im Originaltext durch den Buchstaben, der n Stellen im Alphabet weiter hinten (rechts) steht.
- Entschlüsselungsanweisung: Ersetze jeden Buchstaben im verschlüsselten Text durch den Buchstaben, der n Stellen im Alphabet weiter vorne (links) steht.
- Schlüssel: n (natürliche Zahl zwischen 0 und 26)
- Beispiel
  - Originaltext: "VENI VIDI VICI", Schlüssel = 3
  - verschlüsselter Text: "YHQL YLGL YLFL"
- **Cäsar-Scheibe**



Beide Partner (Sender und Empfänger) kennen einen geheimen Schlüssel, der zum Ver- und zum Entschlüsseln verwendet wird. Eine Kenntnis des Schlüssels erlaubt Zugriff auf die Daten.



Austausch des geheimen Schlüssels über einen anderen, sicheren Kommunikationskanal (z.B. persönlich, Brief)

Für jede mögliche Verbindung wird ein eigener Schlüssel benötigt (Falls derselbe Schlüssel für Nachrichten an B und C benutzt wird, könnte C Nachrichten an B lesen).

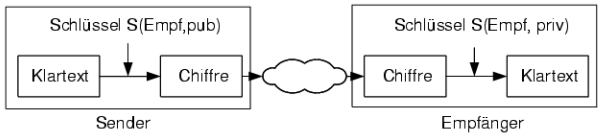
Beispiele: DES, Tripple DES, IDEA

Animation Symmetrische Verschlüsselung

Erweiterte Caesar-Chiffre

Generated by Targeteam

Zum Ver- und Entschlüsseln wird ein Schlüsselpaar (priv, pub) verwendet. Es existiert ein personenbezogener ***privater Schlüssel*** priv und ein ***öffentlicher Schlüssel*** pub, der allgemein zugänglich und jedem bekannt sein darf. Alle Nachrichten, die mit einem Schlüssel codiert (chiffriert) worden sind, können mit dem jeweils anderen Schlüssel wieder decodiert (dechiffriert) werden.



Für sicheren Datenaustausch wird die Nachricht mit dem öffentlichen Schlüssel des Empfängers S(Empf, pub) verschlüsselt. Dann hat nur der Empfänger selbst mit seinem privaten Schlüssel S(Empf, priv) Zugang zum Inhalt.

Geheimer Schlüssel darf nicht aus dem öffentlichen Schlüssel ableitbar sein.

Je länger der Schlüssel desto sicherer ist das System (Angriffsmöglichkeit durch Ausprobieren aller möglichen Schlüssel).

Beispiel: RSA (Schlüssellänge für Home: 256 Bit, Standard: 512 Bit, Militär: 1024 Bit)

Verschlüsselung mit asymmetrischen Verfahren ist üblicherweise langsamer als mit symmetrischen Verfahren (RSA etwa um den Faktor 1000 langsamer als DES). Deshalb werden die Verfahren in der Praxis oft kombiniert.

Nutzung des asymmetrischen Kryptoverfahrens zum Austausch des geheimen Schlüssels.

Verschlüsselung

Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.

Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).

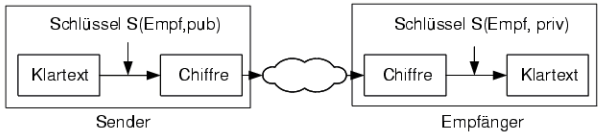
Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.

Symmetrische Verschlüsselung

Asymmetrische Kryptosysteme

Asymmetrische Kryptosysteme

Zum Ver- und Entschlüsseln wird ein Schlüsselpaar (priv, pub) verwendet. Es existiert ein personenbezogener ***privater Schlüssel*** priv und ein ***öffentlicher Schlüssel*** pub, der allgemein zugänglich und jedem bekannt sein darf. Alle Nachrichten, die mit einem Schlüssel codiert (chiffriert) worden sind, können mit dem jeweils anderen Schlüssel wieder decodiert (dechiffriert) werden.



Für sicheren Datenaustausch wird die Nachricht mit dem öffentlichen Schlüssel des Empfängers S(Empf, pub) verschlüsselt. Dann hat nur der Empfänger selbst mit seinem privaten Schlüssel S(Empf, priv) Zugang zum Inhalt.

Geheimer Schlüssel darf nicht aus dem öffentlichen Schlüssel ableitbar sein.

Je länger der Schlüssel desto sicherer ist das System (Angriffsmöglichkeit durch Ausprobieren aller möglichen Schlüssel).

Beispiel: RSA (Schlüssellänge für Home: 256 Bit, Standard: 512 Bit, Militär: 1024 Bit)

Verschlüsselung mit asymmetrischen Verfahren ist üblicherweise langsamer als mit symmetrischen Verfahren (RSA etwa um den Faktor 1000 langsamer als DES). Deshalb werden die Verfahren in der Praxis oft kombiniert.

Nutzung des asymmetrischen Kryptoverfahrens zum Austausch des geheimen Schlüssels.

Generated by Targeteam

Verschlüsselung

Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.

Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).

Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.

Symmetrische Verschlüsselung

Asymmetrische Kryptosysteme

Generated by Targeteam

Allgemeine Möglichkeiten

Prüfe etwas, das die Person weiß (z.B. Passwort)

Prüfe etwas, das die Person besitzt (z.B. Ausweis, Chipkarte)

Prüfe eine physikalische Charakteristik der Person (z.B. Fingerabdruck)

Prüfe Ergebnis einer unbewussten Aktion der Person (z.B. Unterschrift)

Grundproblem bei digitaler Übermittlung von Passworten oder anderen Identitätsbeweisen in verteilten Systemen ist die Kopierbarkeit. Mögliche Lösungen sind:

Verschlüsselte Übermittlung des Passworts (immer noch kopierbar ...)

Eine andere Möglichkeit ist die "digitale Unterschrift".

Digitale Unterschrift

Digitale Unterschrift

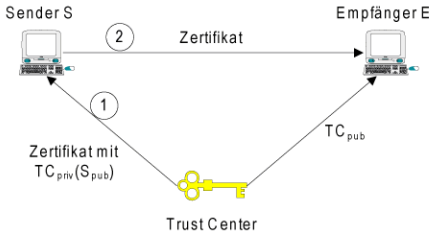
Durch Senden eines, mit dem privaten Schlüssel verschlüsseltem Datums kann man sich eindeutig ausweisen (eine Entschlüsselung ist nur mit dem öffentlichen Schlüssel der Person möglich).

Digitale Unterschrift = Name oder das Paar [Name, Zeitstempel] mit privatem Schlüssel verschlüsselt

Probleme mit sicherem Austausch von öffentlichen Schlüsseln.

Zertifikate

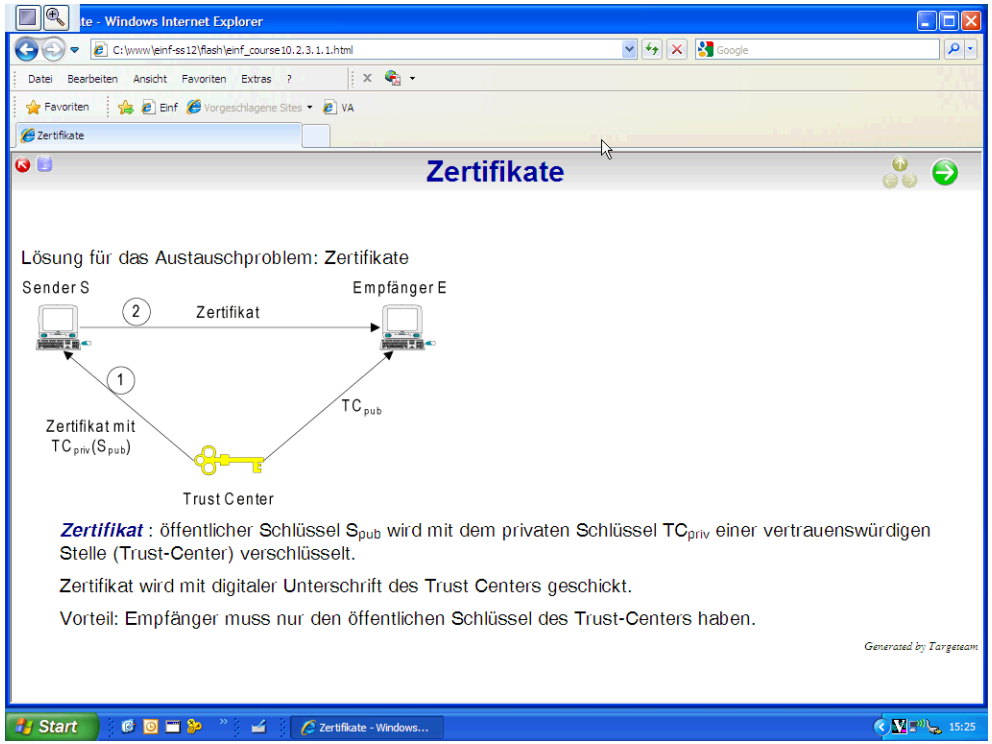
Lösung für das Austauschproblem: Zertifikate



Zertifikat : öffentlicher Schlüssel S_{pub} wird mit dem privaten Schlüssel TC_{priv} einer vertrauenswürdigen Stelle (Trust-Center) verschlüsselt.

Zertifikat wird mit digitaler Unterschrift des Trust Centers geschickt.

Vorteil: Empfänger muss nur den öffentlichen Schlüssel des Trust-Centers haben.



Darstellung von Information

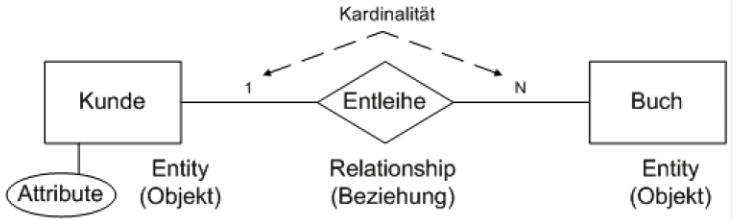
Dieser Abschnitt beschäftigt sich mit Information und ihrer Darstellung im Computer

Information und Nachrichten

Bits und Bytes

Generated by Targeteam

Entity-Relationship-Modell eignet sich zur Darstellung des Datenbankschemas.



Graphisches Hilfsmittel zur semantischen Modellierung eines Anwendungsgebietes, d.h. zum Entwurf einer Datenbank, unabhängig vom konkreten DBS.

Grundidee: Reale Welt (Mini-Welt) läßt sich durch Objekte und Beziehungen zwischen Objekten beschreiben (Objekte: Entities, Beziehungen: Relationships).

Gleichartige Entities (Objektinstanzen) werden zu Entity-Typen (vergleichbar Klassen) bzw. Relationships zu Relationship-Typen zusammengefasst.

Relationales Modell

Schema : legt die Struktur der in der Datenbank gespeicherten Daten fest.
Darstellung mit Hilfe von Relationen

Relation R ⊆ Wertebereich (Attribut 1) * ... * Wertebereich (Attribut n)

- Beispiel der Relation Telefonbuch

  Telefonbuch ⊆ Text * Text * Zahl

  Darstellung als Schema

  Telefonbuch: {[Name: Text, Adresse: Text, ***Telefonnr: Zahl***]}

- Relationale Darstellung von Entity-Typen:

  Kunde: {[***Kundennr: Zahl*** , Vorname: Text, Nachname: Text, Ort: Text]}

  Kundennr ist der Primärschlüssel zur Identifizierung der einzelnen Kunden.

- Relationale Darstellung von Relationship-Typen:

  entleiht: {[***Kundennr: Zahl*** , ***Inventarnr: Zahl*** , Datum: Datum]}

  Kundennr und Inventarnr dient zur Identifizierung eines Entleihvorgangs.

Tabellendarstellung

In relationalen Datenbanken "sieht" der Benutzer die Information in Form von Tabellen (Relationen). Jede dieser Tabellen besteht aus Zeilen und Spalten; Spalten repräsentieren die Attribute von Entities.

Daten in Menge von Tabellen (Relationen) gespeichert. Meist eine Tabelle je Entity-Typ und eine Tabelle je Relationship-Typ.

Je Tabelle: Name, Spalten, Zeilen.

Je Zeile: ein zusammengehöriger Datensatz (Tupel einer Relation). Spalten als "Attribute" bezeichnet.

Jede Tabelle hat "Primärschlüssel": identifiziert Zeilen (Datensätze) eindeutig.

z.B. jeder einzelner Kunde wird durch Kundennr identifiziert.

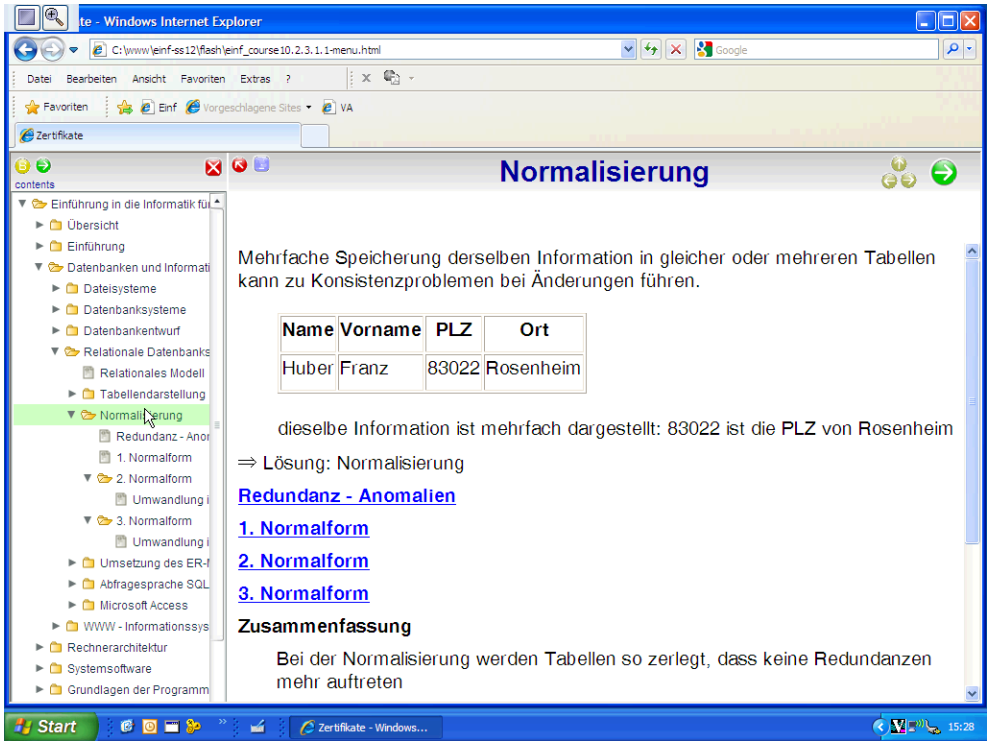
Ordnung der Zeilen irrelevant.

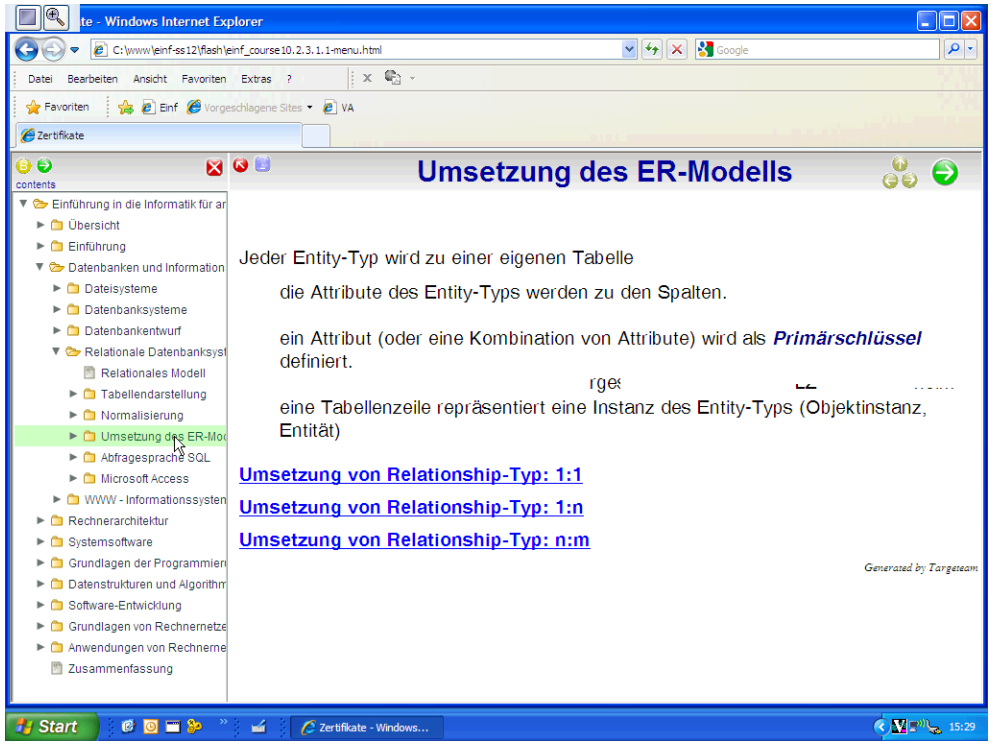
Ordnung der Spalten irrelevant, da durch Namen bezeichnet.

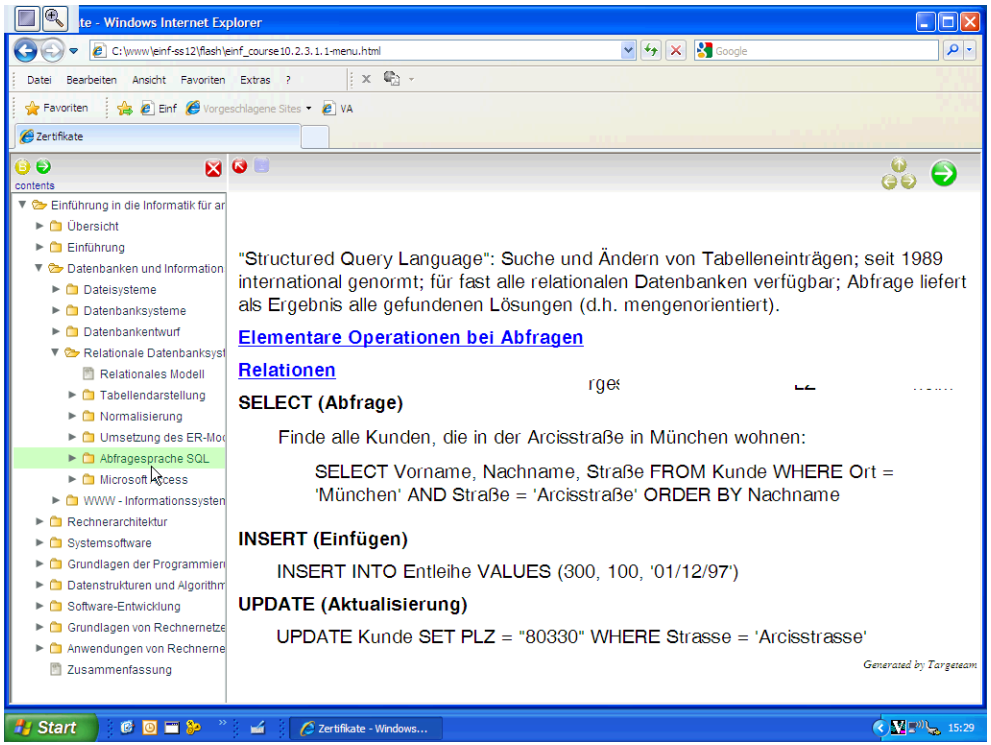
Für Benutzer relevante Informationen: Datenwerte in den Tabellen.

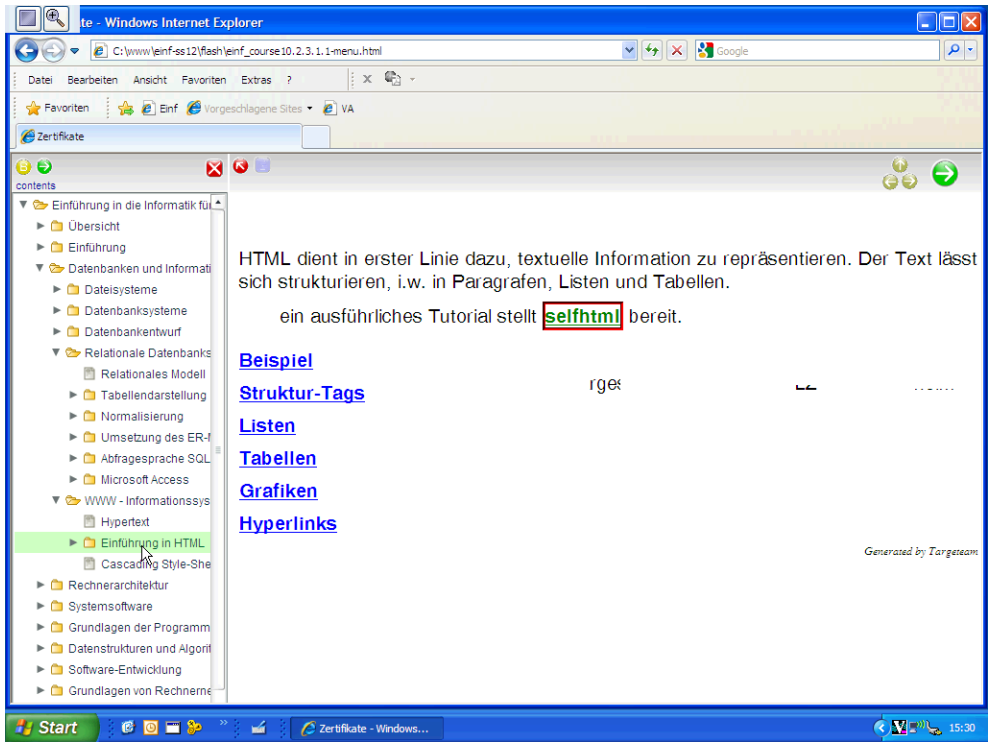
Beziehungen zwischen zwei Tabellen

Beispiel


Normalisierung
Mehrfache Speicherung derselben Information in gleicher oder mehreren Tabellen kann zu Konsistenzproblemen bei Änderungen führen.
Name Vorname PLZ Ort
Huber Franz 83022 Rosenheim
dieselbe Information ist mehrfach dargestellt: 83022 ist die PLZ von Rosenheim
⇒ Lösung: Normalisierung
Redundanz - Anomalien
1. Normalform
2. Normalform
3. Normalform
Zusammenfassung
Bei der Normalisierung werden Tabellen so zerlegt, dass keine Redundanzen mehr auftreten


Umsetzung des ER-Modells
Jeder Entity-Typ wird zu einer eigenen Tabelle
die Attribute des Entity-Typs werden zu den Spalten.
ein Attribut (oder eine Kombination von Attribute) wird als Primärschlüssel definiert.
eine Tabellenzeile repräsentiert eine Instanz des Entity-Typs (Objektinstanz, Entität)
Umsetzung von Relationship-Typ: 1:1
Umsetzung von Relationship-Typ: 1:n
Umsetzung von Relationship-Typ: n:m
Generated by Targeteam


"Structured Query Language": Suche und Ändern von Tabelleneinträgen; seit 1989 international genormt; für fast alle relationalen Datenbanken verfügbar; Abfrage liefert als Ergebnis alle gefundenen Lösungen (d.h. mengenorientiert).
Elementare Operationen bei Abfragen
Relationen
SELECT (Abfrage)
Finde alle Kunden, die in der Arcisstraße in München wohnen:
SELECT Vorname, Nachname, Straße FROM Kunde WHERE Ort = 'München' AND Straße = 'Arcisstraße' ORDER BY Nachname
INSERT (Einfügen)
INSERT INTO Entleihe VALUES (300, 100, '01/12/97')
UPDATE (Aktualisierung)
UPDATE Kunde SET PLZ = "80330" WHERE Strasse = 'Arcisstrasse'
Generated by Targeteam


HTML dient in erster Linie dazu, textuelle Information zu repräsentieren. Der Text lässt sich strukturieren, i.w. in Paragrafen, Listen und Tabellen.
ein ausführliches Tutorial stellt selfhtml bereit.
Beispiel
Struktur-Tags
Listen
Tabellen
Grafiken
Hyperlinks
Generated by Targeteam

Cascading Style-Sheets (CSS)

Festlegung der Formateigenschaften von HTML-Tags

interpretieren durch den Browser zum Formatieren und Positionieren von HTML -Elementen auf dem Nutzerrechner.

Einbettung von CSS-Formaten in die Web-Seite oder als separate Datei, die von Web-Seite referenziert wird.

Eigenschaften werden mit Hilfe von Regeln spezifiziert, eine Regel besteht aus Selektor, der Eigenschaft sowie dem ihr zugewiesenen Wert.

Beispiel

```
BODY { font-size: 20px;
   font-family: Helvetica;
   margin-left: 0.5em}
TD { font-family: inherit; font-size: 20px;
   vertical-align: top; }
P { font-family: Helvetica;
   font-size: 20px;
```

Befehlsvorrat

Transportbefehle

z.B. LOAD, STORE. LOAD: Transportieren von Daten vom Arbeitsspeicher in ein Register; STORE spezifiziert den umgekehrten Weg.

Arithmetische und logische Befehle

z.B. ADD, SUB, AND, OR, CMP

Schiebebefehle

z.B. SH (Shift links, rechts), ROT (Schieben im Kreis)

Sprungbefehle

z.B. JMP (Jump), JGT (Jump Greater Than) - (bedingte) Änderung der Ablaufreihenfolge

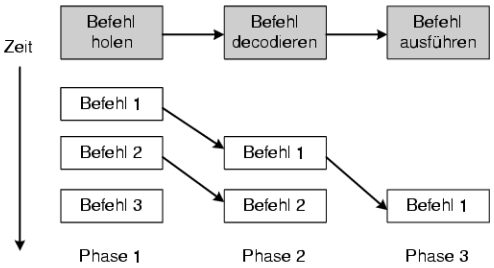
Sonderbefehle

Behandlung von Unterbrechungen (z.B. Alarm bei Division durch 0), Änderungen des Maschinenstatus, Rückmeldungen von E/A Geräten, Laden von Prozessbeschreibungen, Synchronisationsbefehle bei Speicherzugriff etc.

Generated by Targeteam

Fließband Bearbeitung (Pipelining)

Bearbeitung jeden Befehls in mehreren Phasen. Überlappende Verarbeitung. Quasi-parallele Ausführung mehrerer Maschinenbefehle.



Pipelining Animation

Generated by Targeteam

Zweierkomplement-Darstellung

Eine negative Zahl mehr als positive Zahlen. Einfache Umsetzung von Addition und Subtraktion.

Beispiel für 4 bit Darstellung

Formel für Wert einer Zweierkomplement-Zahl

$$W = -b_0 \times 2^{n-1} + \sum_{i=1}^{n-1} \left(b_i \times 2^{n-1-i}\right)$$

mit $b_i \in \{0,1\}$. n ist hier die Anzahl der Bitstellen.

Beispiel

Wert der Zahl W: -1

Binärdarstellung mit 4 Bit: 1111

$$W = -2^3 + 2^2 + 2^1 + 2^0 = -8 + 7 = -1$$

Rechnen mit Zweierkomplement-Zahlen

Generated by Targeteam

Negativbildung und Grundrechenarten sind einfach durchführbar.

Negativbildung einer Zahl

Komplementbildung (Bits invertieren) und 1 addieren.

Beispiel

Zweierkomplement-Codierung mit 8 Bit für -14:

14 =	00001110
Komplement:	11110001
1 addiert:	11110010

Addition von zwei Zahlen

Stellenweise mit Übertrag, analog zum Dezimalsystem.

Differenzbildung von zwei Zahlen

Realisierbar durch Addition mit negativer Zahl.

Codierung von Text

Alphanumerische Daten - ISO-ASCII 8-bit-Code

Darstellung von Buchstaben und Ziffern in einer 8-Bit Folge, d.h. wie Zahl zwischen 0 und 255.

ISO = International Standards Organisation

ASCII = American Standard Code for Information Interchange

Kleinbuchstaben sind in alphabetischer Reihenfolge durchnummeriert (97 - 122)

Großbuchstaben sind in alphabetischer Reihenfolge durchnummeriert (65 - 90)

Ziffern 0 bis 9 sind in aufsteigender Reihenfolge dargestellt (48 - 57)

Darstellung von Sonderzeichen, z.B. CR (Carriage Return = Absatzende), LF (Linefeed = Neuzeile)

Zu den entsprechenden Zeichen des ASCII Codes wird der jeweilige Zahlenwert zur Basis 10 angegeben.

Zeichen Dezimal Binärdarstellung

Rastergrafik - Bilder

Problem: Information gleichmäßig über Fläche verteilt.

Auflösung in Rasterpunkte. Bildschirm: 60 bis 360 Bildelemente (Pixel) pro Zoll (2,54cm)

Darstellung Eigenschaft eines Pixels (Grauwert, Farbe, Helligkeit): meist ein oder zwei Byte)

Darstellung Farbinformation: RGB (rot-grün-blau) oder andere Codierungen

SVGA: 1024 * 768 * (8 bit pro Pixel / 8 bit pro Byte) = 786432 Byte

Graphics Interchange Format (GIF): häufig vorkommende Folgen von Bytes werden in Tabelle eingetragen; im Bild Verweis auf Tabelleneintrag.

The rain in Spain falls mainly on the plain, while the rain in the Amazon just falls ⇒ 85 Zeichen

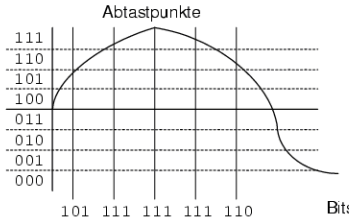
Abkürzungen: W = the, X = ain, Y = on, Z = falls

W rX in SpX Z mXly Y W plX, while W rX in W AmazY just Z ⇒ 57 Zeichen

Joint Photographic Expert Group (JPG): Farben des Bildes werden analysiert;

Töne

Information gleichmäßig über Zeitdauer verteilt.



Diskretisierung, Digitalisierung. 100, 1000 und mehr Werte pro Sekunde.

Darstellung der Eigenschaften des Tonelements durch ein oder zwei Byte

Sprache wird beim Telefon 8000 mal pro Sekunde (8kHz) abgetastet.

Generated by Targeteam

Vererbung

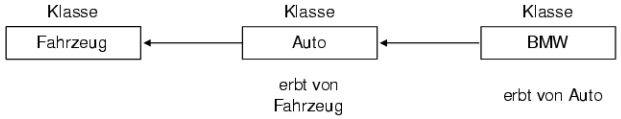
Werkzeug zum Organisieren und Konstruieren von Klassen; Wiederverwendung.

Definition - Vererbung

Seien K und K_i , i = 1,..,n Klassen; Vererbung ist eine Beziehung zwischen K und den K_i , wobei Struktur und Verhalten von K durch Struktur und Verhalten der K_i bestimmt wird; K "erbt" von den Klassen K_i ;

Beziehung zwischen Klassen; K Unterklasse (Subklasse) von K_i ; K_i Oberklasse (Superklasse) von K;

Unterklassen übernehmen Eigenschaften (Attribute, Operationen und Beziehungen) der Oberklasse(n); ggf. über mehrere Stufen. Betrifft Attribute und Methoden;



Einfachvererbung: eine Klasse hat nur eine direkte Oberklasse, d.h. n=1.

Suchverfahren

Gegeben: Menge von Datensätzen. Gesucht: Datensatz mit bestimmter Eigenschaft.

Mengen von Datensätzen

Üblicherweise in Reihung oder Liste gespeichert.

Annahme für die folgenden Verfahren: Daten in einer Reihung gespeichert.

Lineare Suche

Binäre Suche

Suchverfahren Animation

Generated by Targeteam

lirek berklasse, d.

Binäre Suche

Voraussetzung: Ordnung auf Datenelementen. Entsprechend der Ordnung in der Reihung gespeichert (aufsteigend oder absteigend).

Sei int A[n] eine Reihung mit n Elementen, das aufsteigend sortiert ist.

Gesucht wird ein Element mit dem Wert x; gesucht wird x im Bereich A[0] bis A[n-1].

1. wähle m zwischen 0 und n-1; man wird m ungefähr in der Mitte zwischen 0 und n-1 wählen.
2. wenn A[m] == x, dann sind wir fertig, gib m als Ergebnis aus.
3. wenn x < A[m], dann suche weiter im Bereich A[0] bis A[m-1];
4. wenn x > A[m], dann suche weiter im Bereich A[m+1] bis A[n-1]

Doppelte Zahl von Elementen: ein zusätzlicher Vergleich. Bei linearer Suche: Verdopplung des Aufwandes.

lirek berklasse, d.

Generated by Targeteam

Beispiel

Karin	Jim	Bernd	Bernd	Bernd
Franz	Franz	Franz	Franz	Franz
Bernd	Bernd	Jim	Jim	Jim
Jochen	Jochen	Jochen	Jochen	Jochen
Sepp	Sepp	Sepp	Karin	Karin
Jim	Karin	Karin	Sepp	Maria
Maria	Maria	Maria	Maria	Sepp

Generated by Targeteam

se, d.

Komplexität

Algorithmus kann Aufwand erfordern, der"nicht vertretbaren" ist. Bei algorithmischer Lösung eines Problems ist daher auch Effizienz wesentlich.

Komplexität von Algorithmen

Ein Algorithmus ist umso effizienter, je geringer der Aufwand zu seiner Abarbeitung ist.

Aufwand bezieht sich auf bestimmte Ressourcen, z.B. Rechenzeit, Speicherplatz, Anzahl der Geräte

Je nach Ressource verschiedene Komplexitätsmaße. Wichtigste: Zeitkomplexität, Speicherplatzkomplexität.

Zu unterscheiden: Komplexität eines Algorithmus / eines Problems. Problem: zu erreichendes Ziel. Algorithmus: Vorgehen. Komplexität Problem = Komplexität effizientester bekannter Algorithmus.

Komplexitätsmaß für Algorithmus: Funktion abhängig von Größe der Eingabe. Misst Aufwand der Verarbeitung relativ zur zu verarbeitenden Information.

Beispiel

Komplexitätsklassen

Relative Größenordnung (abzüglich konstanter Faktor) in Abhängigkeit von Zahl n der Wertelemente (bestimmt durch Kontext, z.B. Anzahl der Eingabeelemente, Anzahl der zu untersuchenden Datenelemente).

Definition

Sei f: N → N eine Funktion. Die Komplexitätsklasse O(f) ist definiert durch:

$O(f) := \{ g: N \to N \mid \exists\ c > 0, m \geq 0: \forall\ n > m: 0 \leq g(n) \leq cf(n) \}$

O-Notation dient dazu, das asymptotische Wachstum einer Funktion abzuschätzen.

- Sei t(n) die Funktion zur Bestimmung der Laufzeit des Programms.
- mit wachsendem n gewinnt die höchste Potenz von n in t(n) an Bedeutung.

Übliche Komplexitätsklassen

Nicht-polynomiale Probleme gelten als "hart".

Generated by Targeteam

Übliche Komplexitätsklassen

Hauptsächlich verwendete Komplexitätsklassen

logarithmisch O(log n)

linear O(n)

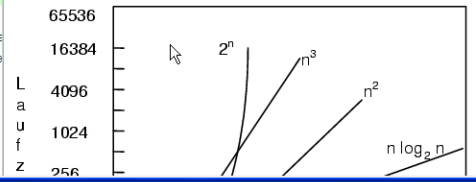
O(n) ⇒ Komplexität ist z.B. 3n + 10;

überlinear O(n log n)

quadratisch $O(n^2)$

polynomial $O(n^k)$, k > 2

exponentiell $O(k^n)$, k >= 2



Komplexität

Algorithmus kann Aufwand erfordern, der"nicht vertretbaren" ist. Bei algorithmischer Lösung eines Problems ist daher auch Effizienz wesentlich.

Komplexität von Algorithmen

Ein Algorithmus ist umso effizienter, je geringer der Aufwand zu seiner Abarbeitung ist.

Aufwand bezieht sich auf bestimmte Ressourcen, z.B. Rechenzeit, Speicherplatz, Anzahl der Geräte

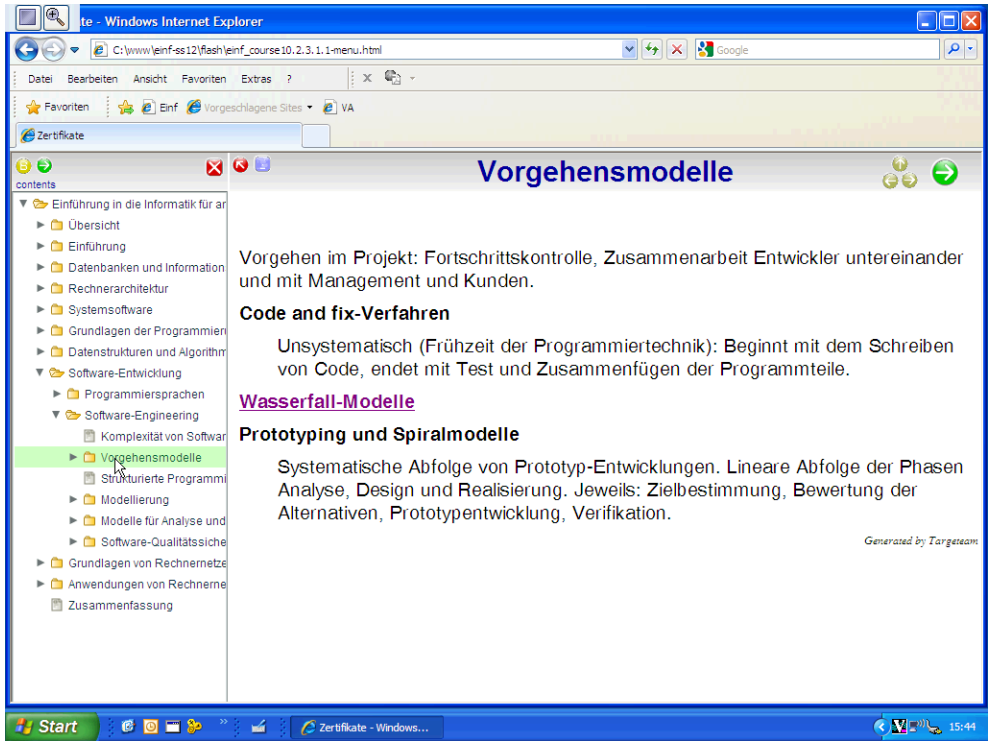
Je nach Ressource verschiedene Komplexitätsmaße. Wichtigste: Zeitkomplexität, Speicherplatzkomplexität.

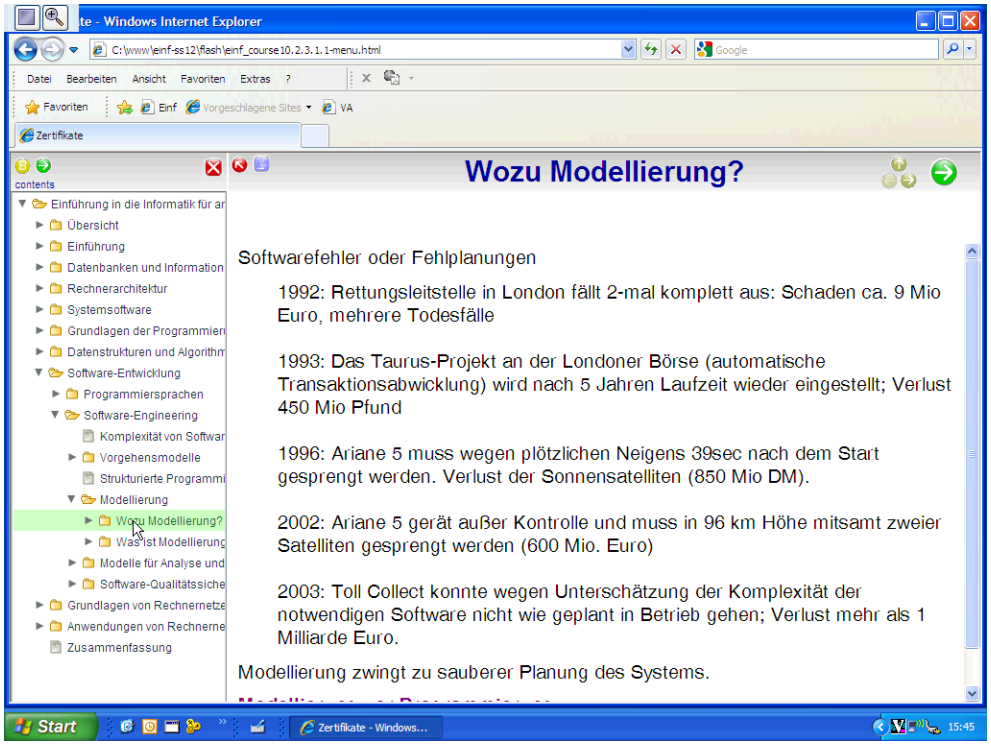
Zu unterscheiden: Komplexität eines Algorithmus / eines Problems. Problem: zu erreichendes Ziel. Algorithmus: Vorgehen. Komplexität Problem = Komplexität effizientester bekannter Algorithmus.

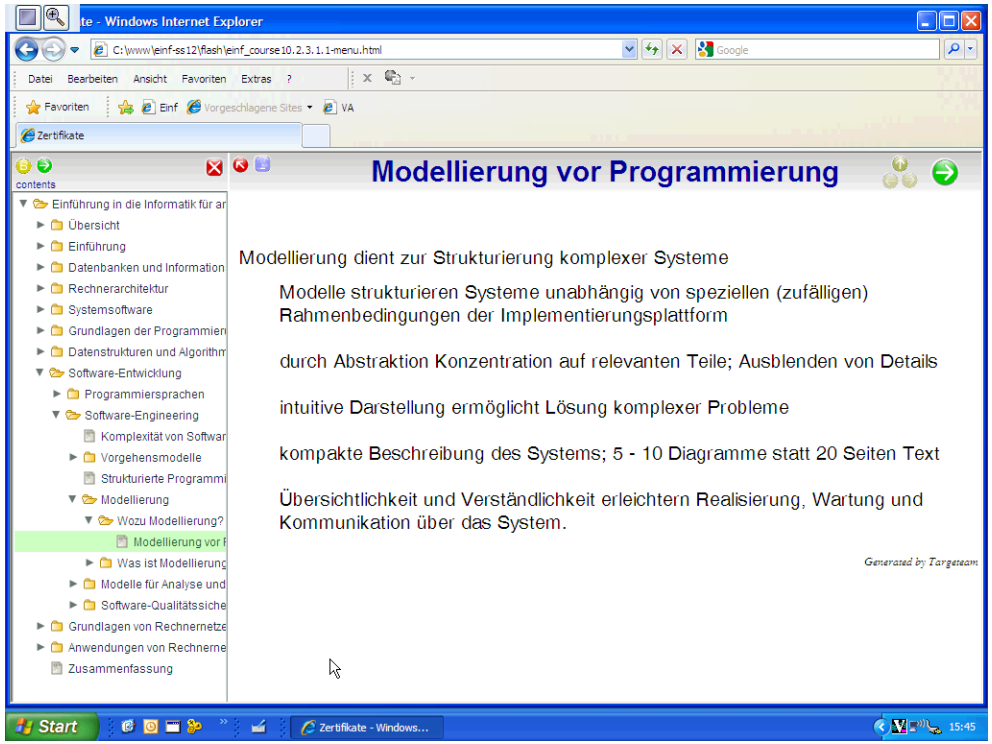
Komplexitätsmaß für Algorithmus: Funktion abhängig von Größe der Eingabe. Misst Aufwand der Verarbeitung relativ zur zu verarbeitenden Information.

Beispiel


Komplexität von Software-Projekten
Maße für den Umfang von Software
Zahl der Quelltextzeilen der Programme, aus denen das Softwareprodukt besteht (LOC = Lines of Code).
Zeit, die benötigt wird, um eine Programm zu erstellen (Messung in Bearbeiter-Jahre (BJ)).
Klassifikation von Software-Projekten
Projektklasse | Quelltext-Zeilen (LOC) | Bearbeitungsaufwand (BJ)
sehr klein | 1 - 1.000 | 0 - 0,2
klein | 1.000 - 10.000 | 0,2 - 2
mittel | 10.000 - 100.000 | 2 - 20
groß | 100.000 - 1 Mio. | 20 - 200
sehr groß | 1 Mio - ... | 200 - ...
Beispiele


Vorgehensmodelle
Vorgehen im Projekt: Fortschrittskontrolle, Zusammenarbeit Entwickler untereinander und mit Management und Kunden.
Code and fix-Verfahren
Unsystematisch (Frühzeit der Programmiertechnik): Beginnt mit dem Schreiben von Code, endet mit Test und Zusammenfügen der Programmteile.
Wasserfall-Modelle
Prototyping und Spiralmodelle
Systematische Abfolge von Prototyp-Entwicklungen. Lineare Abfolge der Phasen Analyse, Design und Realisierung. Jeweils: Zielbestimmung, Bewertung der Alternativen, Prototypentwicklung, Verifikation.
Generated by Targeteam


Wozu Modellierung?
Softwarefehler oder Fehlplanungen
1992: Rettungsleitstelle in London fällt 2-mal komplett aus: Schaden ca. 9 Mio Euro, mehrere Todesfälle
1993: Das Taurus-Projekt an der Londoner Börse (automatische Transaktionsabwicklung) wird nach 5 Jahren Laufzeit wieder eingestellt; Verlust 450 Mio Pfund
1996: Ariane 5 muss wegen plötzlichen Neigens 39sec nach dem Start gesprengt werden. Verlust der Sonnensatelliten (850 Mio DM).
2002: Ariane 5 gerät außer Kontrolle und muss in 96 km Höhe mitsamt zweier Satelliten gesprengt werden (600 Mio. Euro)
2003: Toll Collect konnte wegen Unterschätzung der Komplexität der notwendigen Software nicht wie geplant in Betrieb gehen; Verlust mehr als 1 Milliarde Euro.
Modellierung zwingt zu sauberer Planung des Systems.


Modellierung vor Programmierung
Modellierung dient zur Strukturierung komplexer Systeme
Modelle strukturieren Systeme unabhängig von speziellen (zufälligen) Rahmenbedingungen der Implementierungsplattform
durch Abstraktion Konzentration auf relevanten Teile; Ausblenden von Details
intuitive Darstellung ermöglicht Lösung komplexer Probleme
kompakte Beschreibung des Systems; 5 - 10 Diagramme statt 20 Seiten Text
Übersichtlichkeit und Verständlichkeit erleichtern Realisierung, Wartung und Kommunikation über das System.
Generated by Targeteam

Diagrammtypen

Klassendiagram: spezifiert die Objektklassen (Entitätstypen) und deren hierarchischen Zusammenhänge.

z.B. Auto ist eine Unterklasse von Fahrzeug.

statisches Beziehungsdiagramm: modelliert die statischen Beziehungen zwischen Objekten.

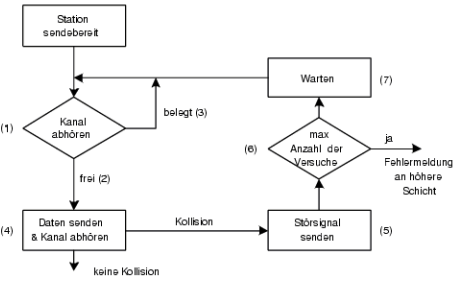
Assoziation: gleichrangige Beziehung zwischen Objekten, z.B. einem Menschen und einer Menge von Büchern, die er liest.

Aggregation: Zusammensetzung eines Objektes aus einer Menge von Einzelteilen, z.B. eine Stadt hat eine Menge Häuser.

Zustandsdiagramm: modelliert die Zustände von Objekten und wie sie von einem Zustand in den nächsten übergehen.

Anwendungsfalldiagramm (Use Case): zeigt den Zusammenhang zwischen Anwendungsfällen und den daran beteiligten Akteuren.

z.B. eine Arztpraxis hätte die Akteure Arzt, Arzthelfern und Patient sowie die Anwendungsfälle: Patient anmelden, Diagnose stellen und Abrechnung.

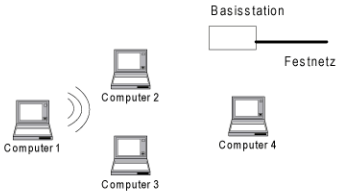


1. Sendewillige Station (Rechner) überwacht Übertragungsmedium (Bus)
2. Übertragungsmedium frei, dann kann Übertragung beginnen
3. Während der Übertragung wird Kanal simultan abgehört; falls gesendete Information und abgehörte Information unterschiedlich, dann wurde eine Kollision festgestellt, d.h. ein anderer Rechner hat auch mit der Übertragung begonnen.

Wireless LAN

verwenden i.a. eine modifizierte Form von CSMA/CD ⇒ CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).

alle Rechner eines bestimmten drahtlosen LAN senden auf der gleichen Funkfrequenz (z.B. 2,4 Ghz Bereich).



Ablauf des Verfahrens, falls Computer 1 an Computer 2 senden möchte.

Computer 1 überprüft, ob gerade ein anderer Rechner sendet.

falls nein sendet Computer 1 eine Steuernachricht an Computer 2, in dem er seinen Übertragungswunsch kundtut.

Computer 2 antwortet mit einer Steuernachricht an Computer 1, in dem er seine

Bedeutung der Schichten

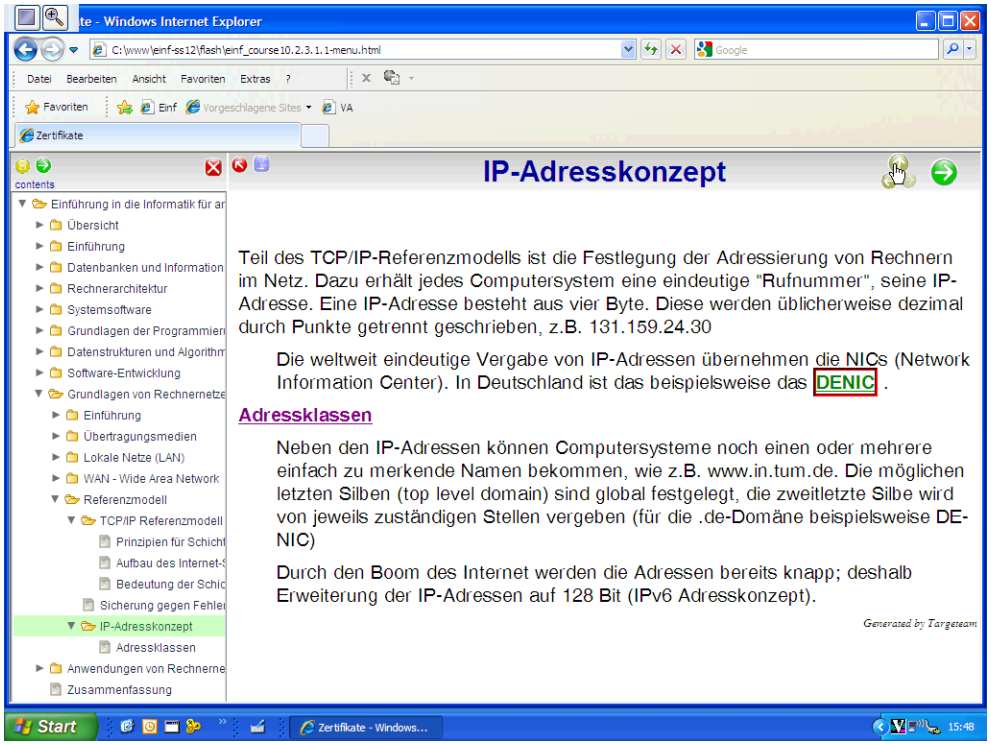
Netzzugriff : bietet eine Übertragungsmöglichkeit einzelner Dateneinheiten (Bits) unter bestimmten Zeitbedingungen an; Nachrichtenübertragung zwischen zwei benachbarten Rechnern.

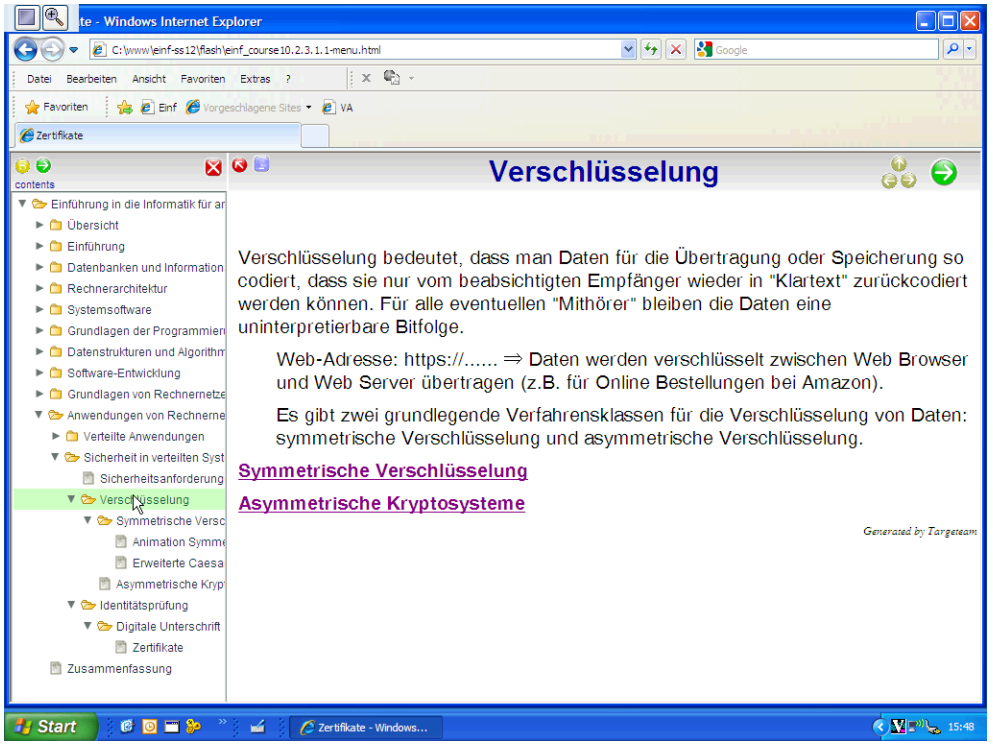
Aufgaben: transparente Übertragung von Bitsequenzen, Berücksichtigung der Eigenschaften der Übertragungsmodi (elektrisch, Lichtwelle), Zusammenfassung von Bitsequenzen zu Rahmen (Frames), Fehlererkennung und Fehlerkorrektur auf Rahmenebene

Internet : fehlerfreie Übermittlung eines Pakets von einem Endrechner, über ein Netz von Routern (Vermittlungsrechnern) hinweg, bis hin zum zweiten Endrechner; beinhaltet Routing und Adressierung; fügt Netzwerk-Header hinzu.

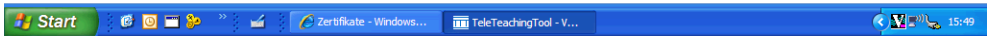
Aufgaben: Zusammenschaltung von Teilstrecken zu einer End-zu-End Verbindung, Wegewahl und Vermittlung, Transporteinheit abhängig von der Vermittlungstechnik (bei Paketvermittlung Verwendung von Paketen)

Transport : fehlerfreier Transport von Nachrichten zwischen zwei kommunizierenden Prozessen auf zwei Endrechnern; bildet die anwendungsorientierten Schichten auf die netz-abhängigen Schichten ab; fügt Transport-Header hinzu.


te - Windows Internet Explorer
C:\www\einf-ss12\flash\einf_course10.2.3.1.1-menu.html
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Zertifikate
contents
Einführung in die Informatik für ar
Übersicht
Einführung
Datenbanken und Information
Rechnerarchitektur
Systemsoftware
Grundlagen der Programmier
Datenstrukturen und Algorithm
Software-Entwicklung
Grundlagen von Rechnernetze
Einführung
Übertragungsmedien
Lokale Netze (LAN)
WAN - Wide Area Network
Referenzmodell
TCP/IP Referenzmodell
Prinzipien für Schicht
Aufbau des Internet-S
Bedeutung der Schic
Sicherung gegen Fehle
IP-Adresskonzept
Adressklassen
Anwendungen von Rechnerne
Zusammenfassung
IP-Adresskonzept
Teil des TCP/IP-Referenzmodells ist die Festlegung der Adressierung von Rechnern im Netz. Dazu erhält jedes Computersystem eine eindeutige "Rufnummer", seine IP-Adresse. Eine IP-Adresse besteht aus vier Byte. Diese werden üblicherweise dezimal durch Punkte getrennt geschrieben, z.B. 131.159.24.30
Die weltweit eindeutige Vergabe von IP-Adressen übernehmen die NICs (Network Information Center). In Deutschland ist das beispielsweise das DENIC .
Adressklassen
Neben den IP-Adressen können Computersysteme noch einen oder mehrere einfach zu merkende Namen bekommen, wie z.B. www.in.tum.de. Die möglichen letzten Silben (top level domain) sind global festgelegt, die zweitletzte Silbe wird von jeweils zuständigen Stellen vergeben (für die .de-Domäne beispielsweise DE-NIC)
Durch den Boom des Internet werden die Adressen bereits knapp; deshalb Erweiterung der IP-Adressen auf 128 Bit (IPv6 Adresskonzept).
Generated by Targeteam
Start
Zertifikate - Windows...
15:48


te - Windows Internet Explorer
C:\www\einf-ss12\flash\einf_course10.2.3.1.1-menu.html
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Zertifikate
contents
Einführung in die Informatik für ar
Übersicht
Einführung
Datenbanken und Information
Rechnerarchitektur
Systemsoftware
Grundlagen der Programmier
Datenstrukturen und Algorithm
Software-Entwicklung
Grundlagen von Rechnernetze
Anwendungen von Rechnerne
Verteilte Anwendungen
Sicherheit in verteilten Syst
Sicherheitsanforderung
Verschlüsselung
Symmetrische Versc
Animation Symme
Erweiterte Caesa
Asymmetrische Kryp
Identitätsprüfung
Digitale Unterschrift
Zertifikate
Zusammenfassung
Verschlüsselung
Verschlüsselung bedeutet, dass man Daten für die Übertragung oder Speicherung so codiert, dass sie nur vom beabsichtigten Empfänger wieder in "Klartext" zurückcodiert werden können. Für alle eventuellen "Mithörer" bleiben die Daten eine uninterpretierbare Bitfolge.
Web-Adresse: https://..... ⇒ Daten werden verschlüsselt zwischen Web Browser und Web Server übertragen (z.B. für Online Bestellungen bei Amazon).
Es gibt zwei grundlegende Verfahrensklassen für die Verschlüsselung von Daten: symmetrische Verschlüsselung und asymmetrische Verschlüsselung.
Symmetrische Verschlüsselung
Asymmetrische Kryptosysteme
Generated by Targeteam
Start
Zertifikate - Windows...
15:48


hingTool - Version 25.10.2009
Student Teacher Post Processing Extras
Help


Start
Zertifikate - Windows...
TeleTeachingTool - V...
15:49