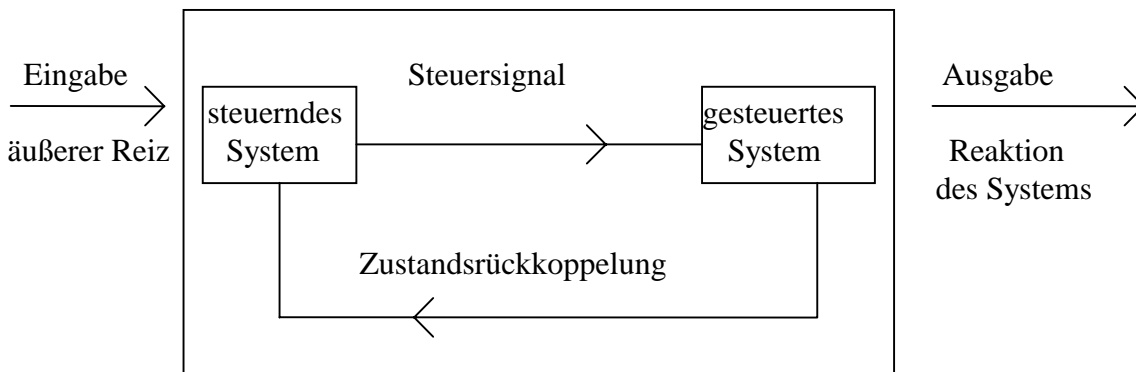


INHALTSVERZEICHNIS

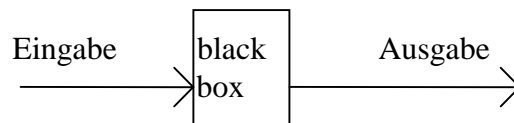
ABGRENZUNG DER INFORMATIK VON DER KYBERNETIK	2
NACHRICHT UND INFORMATION.....	4
DIGITALE NACHRICHTEN.....	5
VERSCHLÜSSELUNGSVERFAHREN.....	9
BETRIEBSSYSTEME.....	10
RECHNERTYPEN	12
AUFBAU EINES COMPUTERSYSTEMS.....	13
PROGRAMMBEFEHLE	14
RECHNEN IM DUALSYSTEM.....	15
DATENSICHERUNG.....	16
DATENSCHUTZGESETZE	16
VOM PROBLEM ZUM PROGRAMM.....	17
PROGRAMMIERAUFGABEN.....	17
ANHANG.....	18

Abgrenzung der Informatik von der Kybernetik

Bei der Entwicklung der *Kybernetik* ging man von realen Steuerungssystemen aus: Nervensystem, Gehirn, Walzstraße, Rechananlage, Industriebetrieb oder Volkswirtschaft. Die mathematische *Kybernetik* befaßt sich mit abstrakten Steuerungssystemen. Untersucht werden die **Gesetzmäßigkeiten** der Struktur und das **Verhalten** von Steuerungssystemen. **Anwendung** kybernetischer Sätze in: Biologie, Medizin, Nachrichtentechnik, Physik. Die Überprüfung solcher Sätze erfolgt durch Herstellen von kybernetischen Modellen. Je nachdem, ob man sich ein abstraktes Steuerungssystem vorstellt als eine Verbindung folgender Art von **steuerndem** und **gesteuertem** System, die jeweils Unterstrukturen aufweisen,



oder als einen schwarzen Kasten (black box), dessen Inneres man nicht kennt,



kommt man zu zwei verschiedenen Methoden:

1) Mikro-Methode

- Untersuchung der Elemente des Systems
- Untersuchung der Verbindung der Elemente untereinander (mit Hilfe der Graphentheorie)

2) Makro-Methode

- Analyse des Informationsflusses
- Analyse des Informationscodes
- Bestimmung der Funktion $\text{Ausgabe} = f(\text{Eingabe})$

Die Black-Box-Philosophie, die der Makro-Methode und der mathematischen Kybernetik zugrunde liegt, ordnet sich in den **Behaviorismus** ein, der nur das Studium von Verhaltensweisen für sinnvoll hält, die von Außenstehenden beobachtet werden können, etwa der Zusammenhang Reiz und Reaktion. Bei der **Modellierung** konkreter Systeme wird also gerade der nicht berechenbare Teil weggelassen, man verkürzt die ursprüngliche Systemkomplexität.

Weitere Anwendungsprobleme sind:

Synthese von Systemen

Umformung von Systemen

Untersuchung der **Zuverlässigkeit** eines Systems.

In der **Informatik** wird die Kybernetik auf **Rechenanlagen** beschränkt, zusätzlich treten weitere Gesichtspunkte auf:

Leistung und **Konstruktion** von Computern. Das Interesse der Informatik (Computer Science) richtet sich auf *Struktur, Wirkungsweise, Fähigkeiten, Verwendungsmöglichkeiten und Konstruktionsprinzipien* von DV-Anlagen.

Die Informatik unterteilt sich in **theoretische**, **technische** und **praktische** Informatik.

Nachricht und Information

Die Zuordnung zwischen **Nachricht** und **Information** ist **nicht** eindeutig.

Bei gegebener **Information** kann es **verschiedene** Nachrichten geben (z.B. in verschiedenen Sprachen).

Ebenso umgekehrt: die Nachricht vom Absturz eines Flugzeuges hat für die Angehörigen eine ganz andere **Bedeutung** als für die Fluggesellschaft.

Zwischen Sender und Empfänger einer Nachricht muß also eine **Interpretationsvorschrift f** verabredet werden, damit aus einer Nachricht **N** die Information **I** interpretiert werden kann

$$I = f(N)$$

Oft ist diese Interpretationsvorschrift nur bestimmten Gruppen bekannt:

Berufssprachen, Jargon, Dialekte, wissenschaftliche Fachsprachen.

Am deutlichsten wird der Zusammenhang *Nachricht - Information* in der **Kryptologie**. Nur wer den Schlüssel kennt, kann der übermittelten Nachricht die Information entnehmen.

Beispiele:

a) *Der Goldkäfer von Edgar Allan Poe*

Mit Hilfe eines verschlüsselten Textes kann ein Schatz gefunden

53%%+305)) 6 " ; 4826) 4% .) 4%) ; 806 " ; 48
+8/60)) 85 ; 1% (; : % " 8+83 (88) 5 " + ; 46 (; 88 "
96 " ? ; 8) "% (; 485) ; 5 " + 2 : "% (; 4956 " 2 (5 " - 4
) 8/8 " ; 4069285) ;) 6+8) 4%% ; 1 (% 9 ; 48
081 ; 8 : 8% 1 ; 48+85 ; 4) 485+528806 " 81 (% 9
; 48 ; (88 ; 4 (% ? 34 ; 48) 4% ; 161 ; : 188 ; % ? ;

Mit einer Häufigkeitsanalyse und der Kenntnis der Häufigkeiten der Buchstaben im englischen Alphabet kommt man zum Ziel. (ETHOSNAIRDFLBMGYUVPCKJWQXZ)

b) bis morgen / see you tomorrow

gleiche Information, aber verschiedene Nachrichten

c) Ta2 - e2 / Desoxyribonukleinsäure

Spezialsprachen: Schach bzw. Chemie

d) Seelöwe gesichtet

als offene Nachricht maskierte Geheimnachricht

e) MOMEBR

Datumsangabe mit Schlüsselwort M I L C H P R O B E

0 1 2 3 4 5 6 7 8 9

JDOOLD HVW RPQLV GLYLVD (lateinisch) oder

OH SDBV GH JDOOHV HVW SDUWDJH (französisch)

Cäsarsubstitution: der dritte nächste Buchstabe des Alphabetes

f) LIRPA oder YAMLRK

Transposition: rückwärts lesen

g) tante anna gestorben + beerdigung uebermorgen + 13. November dinstlaken + emma schubert

als offene Nachricht getarnte Geheimnachricht (bundestag)

h) Komme heute nacht. / Komme heute nicht.

*Sehr geringe Veränderung, aber Information **wesentlich** verändert.*

a - 97 = 01100001 i - 105 = 01101001 **ein** Bit hat sich nur geändert!

Digitale Nachrichten

Ein **Zeichen**¹ ist ein Element einer endlichen Menge von unterscheidbaren „Dingen“, dem **Zeichenvorrat**.

Ein Zeichenvorrat, in dem eine Reihenfolge (lineare Ordnung) für die Zeichen definiert ist, heißt **Alphabet**².

Einige Beispiele von Alphabeten (die Ordnung ist die des Aufzählens) sind:

- Das Alphabet der Dezimalziffern {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}
- Das Alphabet der großen lateinischen Buchstaben {A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}
- Das Alphabet der kleinen griechischen Buchstaben {α, β, γ, δ, ε, ζ, η, θ, ι, κ, λ, μ, ν, ξ, ο, π, ρ, σ, τ, υ, φ, χ, ψ, ω}
- Das Alphabet der großen kyrillischen Buchstaben {А, В, С, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}

Zeichenvorräte ohne eine allgemein akzeptierte Anordnung der Zeichen sind etwa

- Der Zeichenvorrat der internationalen Lautschrift
- Der Zeichenvorrat einer Schreibmaschine
- Der Zeichenvorrat der japanischen **Katakana-Schrift**

ア	カ	サ	タ	ナ	ハ	マ	ヤ	ラ	ワ
A	KA	SA	TA	NA	HA	MA	YA	RA	WA
イ	キ	シ	チ	ニ	ヒ	ミ	リ	ン	
I	KI	SHI	CHI	NI	HI	MI	RI	N	
ウ	ク	ス	ツ	ヌ	フ	ム	ユ	ル	
U	KU	SU	TSU	NU	FU	MU	YU	RU	
エ	ケ	セ	テ	ネ	ヘ	メ		レ	
E	KE	SE	TE	NE	HE	ME		RE	
オ	コ	ソ	ト	ノ	ホ	モ	ヨ	ロ	
O	KO	SO	TO	NO	HO	MO	YO	RO	

- Der Zeichenvorrat der Spielkartenfarben ♣♠♥♦
- Der Zeichenvorrat chinesischer Ideogramme (einige tausend Zeichen)

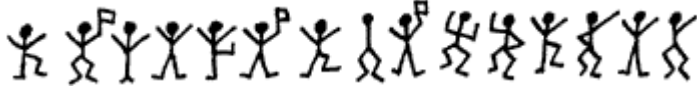
¹ DIN 44300 sagt aus: **Zeichen**: Ein Element aus einer vereinbarten endlichen Menge von Elementen. Die Menge wird **Zeichenvorrat** (character set) genannt.

² DIN 44300 sagt aus: **Alphabet**: Ein (in vereinbarter Reihenfolge) geordneter Zeichenvorrat. Der Unterschied zwischen Alphabet und Zeichenvorrat wird häufig übersehen.

- Der Zeichenvorrat der Braille-Schrift

A B C D E F G H I J K L M N O P Q R S T U
ABCDEFGHI JKLMNOPQRSTU

- Der Zeichenvorrat von Sherlock Holmes



Eine Geheimnachricht aus „The Adventure of the Dancing Man“ von Conan Doyle

- Der Zeichenvorrat des „genetischen Codes“, bestehend aus den vier Buchstaben A, C, G und T, die für die chemischen Verbindungen Adenin, Cytosin, Guanin und Thymin stehen.
- Der Zeichenvorrat des Flexowriter-Codes(8-Bit-Code)

Spur - Nr. (P = Prüfbit) (T = Taktspur)	Lochkombination								
	P	7	6	5	4	T	3	2	1
Zeichen									
Leerzeichen						.			
BS	●				●	.			
0			●	●		.			
1	●		●	●		.			●
2	●		●	●		.		●	
3			●	●		.		●	●
4	●		●	●		.	●		
5			●	●		.	●		●
6			●	●		.	●	●	
7	●		●	●		.	●	●	●
8	●		●	●	●	.			
9			●	●	●	.			●
A		●				.			●
B		●				.		●	
C	●	●				.		●	●
D		●				.	●		
E	●	●				.	●		●
F	●	●				.	●	●	
G		●				.	●	●	●
H		●			●	.			
I	●	●			●	.			●
J	●	●			●	.		●	
K		●			●	.		●	●
L	●	●			●	.	●		
M		●			●	.	●		●
N		●			●	.	●	●	
O	●	●			●	.	●	●	●
P		●		●		.			
O	●	●		●		.			●
R	●	●		●		.		●	
S		●		●		.		●	●
T	●	●		●		.	●		
U		●		●		.	●		●
V		●		●		.	●	●	
W	●	●		●		.	●	●	●
X	●	●		●	●	.			
Y		●		●	●	.			●
Z		●		●	●	.		●	
Löschen einer Irrung	●	●	●	●	●	.	●	●	●

- Der Zeichenvorrat des Morsecodes

a	.-.-.	j	.-.-.-	t	-	0	-.-.-.-
ä	-.-.-	k	-.-.-	u	.-.-	1	.-.-.-
b	-...-	l	.-...-	ü	.-.-.-	2	.-.-.-
c	-.-.-.	m	-.-	v	.-...-	3	.-.-.-
ch	-.-.-.-	n	-.-.	w	.-.-	4	.-.-.-
d	-...-	o	-.-.-	x	-...-	5	.-.-.-
e	.	ö	-.-.-.	y	-.-.-	6	-...-
f	.-.-.	p	.-.-.-	z	-.-.-.	7	-.-.-.
g	-.-.	q	-.-.-	à	.-.-.-	8	-.-.-.
h	.-...-	r	.-.-.	é	.-...-	9	-.-.-.
i	..	s	.-...-	ñ	-.-.-.-		

Punkt	.-.-.-.-	Doppelstrich	-.-.-.-
Komma	-.-.-.-	Trennung	-.-.-.-
Apostroph	.-.-.-.-	Bruchstrich	-.-.-.-
Doppelpunkt	-.-.-.-	Anfangszeichen	-.-.-.-
Bindestrich	-.-.-.-	Schlußzeichen	.-.-.-.
Klammer	-.-.-.-	Verstanden	.-.-.-.
Fragezeichen	.-.-.-.-	Aufforderung zum Senden	-.-.-
Anführungszeichen	.-.-.-.-	Warten	.-.-.-.
Auslassungszeichen	.-.-.-.-	Irrung	.-.-.-.-
Unterstreichung	.-.-.-.-	Notruf (SOS)	.-.-.-.-

- Der Zeichenvorrat des Lochkartencodes

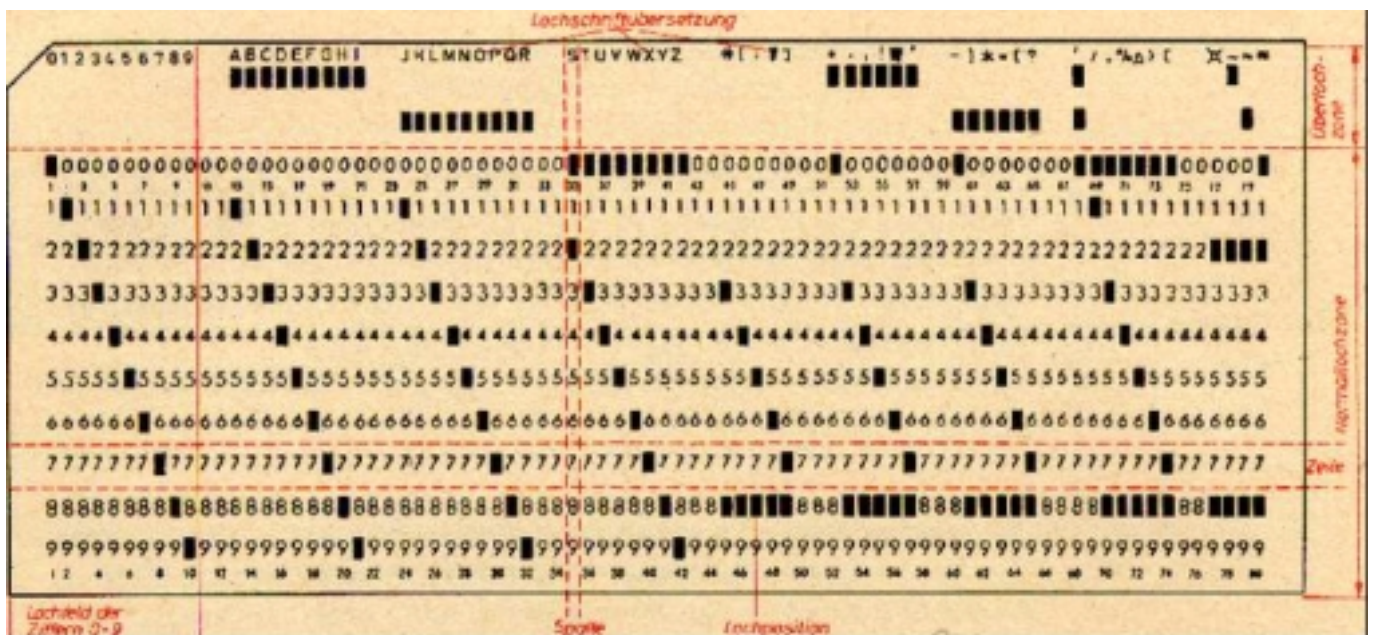


Tabelle zum Lochkartencode

Loch-kombina-tion	Zeichen	Loch-kombina-tion	Zeichen	Loch-kombina-tion	Zeichen	Loch-kombina-tion	Zeichen	Loch-kombina-tion	Zeichen
0	0	7	7	12-5	E	11-3	L	0-2	S
1	1	8	8	12-6	F	11-4	M	0-3	T
2	2	9	9	12-7	G	11-5	N	0-4	U
3	3	12-1	A	12-8	H	11-6	O	0-5	V
4	4	12-2	B	12-9	I	11-7	P	0-6	W
5	5	12-3	C	11-1	J	11-8	Q	0-7	X
6	6	12-4	D	11-2	K	11-9	R	0-8	Y

Binär-codes für Dezimalziffern

Ziffernsymbol	direkt	Gray
0	0000	0000
1	000L	000L
2	00L0	00LL
3	00LL	00L0
4	0L00	0LL0
5	0L0L	0LLL
6	0LL0	0L0L
7	0LLL	0L00
8	L000	LL00
9	L00L	LL0L
Gewichte der Stellen	8421	15 731

Verschlüsselungsverfahren

1) Vigenèreverfahren

Zur Verschlüsselung wird ein Schlüsselwort benötigt, das die Auswahl der 26 möglichen zyklischen Vertauschungen der alphabetischen Anordnung A, B, C, ..., Z steuert (26-facher Cäsar). Um im jeweils ausgewählten Alphabet das richtige Ersetzungssymbol zu finden, benutzt man den sogenannten St.-Cyr Schieber, dessen zwei Teile verschiebbar sind.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
Index

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Zunge

Soll der Text **CODIERUNGSTHEORIE** verschlüsselt werden und lautet das Schlüsselwort **INFORMATIK**, dann stellt man für jeden Buchstaben des Klartextes zusammengehörige Buchstabenpaare auf Index und Zunge untereinander. Der erste Buchstabe des Schlüsselwortes auf der Zunge wird unter das „A“ vom Index gestellt. Unter dem ersten Buchstaben des Textes, der auf dem Index gesucht wird, steht der Codebuchstabe:

ABCDEFGHIJKLMNOPQRSTUVWXYZ ↑ ↓	Index
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ	Zunge

allgemein: den i-ten Buchstaben des Schlüsselwortes *immer* unter das „A“ vom Index stellen, unter dem i-ten Buchstaben des Originaltextes auf dem Index steht der Codebuchstabe.

Auf diese Weise erhält man für den Text **CODIERUNGSTHEORIE** den Codetext

KBIWVDUGOCBUJCIUE! Ist der Text länger als das Schlüsselwort, dann wird wieder von vorn begonnen.

2) Simmelverfahren (aus dem Roman *Und Jimmy ging zum Regenbogen*)

Den Buchstaben des Schlüsselwortes werden Zahlen zugeordnet. Der erste Buchstabe des Alphabetes, der im Schlüsselwort vorkommt, erhält die Zahl 1, usw. Beispiel:

U N D J I M M Y G I N G Z U M R E G E N B O G E N
22 16 2 12 10 13 14 24 6 11 17 7 25 23 15 21 3 8 4 18 1 20 9 5 19

Die Zahlen geben die Verschiebung im Alphabet an. Der i-te Buchstabe des Textes wird im Alphabet um so viele Buchstaben nach rechts verschoben, wie die i-te Zahl angibt. Beim Entschlüsseln wird nach links verschoben. Beispiel:

EIQXSRFSTRLUCTXMNCRYEYBSXNLGZQVTRKDRWRFTWHV	Code
ISOLIERUNGUNDWIRKUNGDESNERVENGIFTESAPSIEBEN	Text

(E=5, 5-22= -17, -17+26=9, I=9)

3) Playfair - Verfahren

Gegeben ist eine Matrix, die die nötigen Zeichen enthält.

Bearbeitet werden immer Buchstabenpaare!

D	B	M	W	I
C	O	X	G	E
Q	Y	R	F	S
Z	A	K	T	P
L	U	H	N	V

Verschlüsselung von a_1 , a_2 in b_1 , b_2

- Sind a_1 und a_2 die zwei diagonal gegenüberliegenden Ecken eines Rechtecks, dann sind b_1 und b_2 die anderen Ecken, wobei b_1 in derselben Zeile steht wie a_1 .
- Sind a_1 und a_2 in derselben Zeile, dann stehen b_1 und b_2 unmittelbar rechts von a_1 bzw. a_2 .
- Sind a_1 und a_2 in derselben Spalte, dann stehen b_1 und b_2 unmittelbar unter a_1 bzw. a_2 .
- Falls $a_1 = a_2$, ersetzt man a_2 durch einen beliebigen, aber vorher vereinbarten Buchstaben (z.B. **Q**). Hat der zu verschlüsselnde Text eine ungerade Länge, fügt man einen beliebigen aber vorher vereinbarten Buchstaben (z.B. **Q**) an.

Beispiel: TECHNISCHEUNIVERSITÄET
PGXLVWQEVXHV EIXSPEPKGP

Betriebssysteme

Zusammenfassende Bezeichnung für alle Programme, die die Ausführung der Benutzerprogramme, die Verteilung der **Betriebsmittel** auf die einzelnen Benutzerprogramme und die Aufrechterhaltung der **Betriebsart** steuern und überwachen. Zur Bewältigung der vielfältigen Aufgaben verfügt das BS über zahlreiche Komponenten, die jeweils eine oder mehrere Teilaufgaben wahrnehmen. Die drei wichtigsten Komponenten sind Organisations-, Dienst- und Übersetzungsprogramme.

Organisationsprogramme

In der **Speicherverwaltung** übernehmen sie die Lösung der folgenden Aufgaben:

- Kontrolle aller im System vorkommenden Speicher
- Zuteilung von Speicher an Benutzerprogramme
- Organisation von **Speicherhierarchien**
- Kommunikation mit anderen RA

Die Organisationsprogramme der **Prozessorverwaltung** veranlassen die Zuteilung des Prozessors an eines der zu bearbeitenden Programme.

Die Organisationsprogramme der **Geräteverwaltung** koordinieren

- die Auswahl und Bereitstellung der für **Eingabe** und **Ausgabe** geeigneten Geräte entsprechend den Anforderungen der Benutzerprogramme
- die Anpassung an die speziellen physikalischen Eigenschaften der Geräte
- die Überwachung der Datenübertragung zwischen Programm und Gerät
- die Datenübertragung in **Datennetzen** (elektronische Post, Internet)

Dienstprogramme

Diese lösen Standardanwendungsprobleme. Typische Dienstprogramme sind Sortierprogramme, Dateiverwaltungsprogramme, Lader, Binder, Editor, Debugger.

Hinzu kommen Statistik- und Abrechnungsprogramme, um die Auslastung der Geräte oder die Benutzergebühren zu ermitteln.

Zusätzliche Anforderungen an BS entstehen, wenn die Komponenten des BS über verschiedene Rechner verteilt sind. Zur Kommunikation mit dem BS dient eine Kommandosprache, mit ihrer Hilfe kann der Benutzer Aufträge formulieren.

Übersetzungsprogramme

Diese übersetzen Programme höherer Programmiersprachen in auf einer RA ausführbare Programme.

Die Leistungsfähigkeit einer RA hängt entscheidend von einer effizienten Implementierung der Betriebssystemkomponenten ab. Dies ist keine leichte Aufgabe, denn der Speicherbedarf liegt häufig bei mehreren Millionen Bytes, selbst bei PC's beträgt er oft mehr als 256000 Bytes.

Drei auf Großrechnern verbreitete BS sind

- VM (auf IBM- und dazu kompatiblen Rechnern)
- BS 2000 (auf Siemens-Rechnern)
- UNIX (auf den meisten Rechnern verfügbar)

Das BS **VM** bietet jedem Benutzer eine eigene virtuelle Maschine mit eigenem Betriebssystem an. Beispiele für solche BS sind **DOS** (disk operating system), **MVT** (multiprogramming with a variable number of tasks), **MVS** (multiple virtual storage). Auf dem Rechner können also gleichzeitig mehrere BS nebeneinander ablaufen, wobei jeder Benutzer sich aus einer gegebenen Menge von BS seines auswählt. Das System **VM** besteht aus zwei großen Komponenten: dem Kontrollprogramm **CP**, das die virtuellen Maschinen überwacht und die Betriebsmittel verwaltet, und der Interaktionskomponente **CMS** (conversational monitoring system), die die Dialoganteile und die speziellen Funktionen eines Terminals umfaßt.

BS 2000 unterstützt den Teilnehmerbetrieb und die virtuelle Adressierung. Das System unterteilt sich in einen zentralen Teil, das Organisationsprogramm und die Benutzerprogramme.

UNIX ist mittlerweile in verschiedenen Versionen auf fast allen Rechnern verfügbar. Der zentrale Teil (cernal) ist in der Programmiersprache C geschrieben, so daß er relativ leicht auf die verschiedensten Computer übertragen werden kann. Wesentlich für UNIX sind das **hierarchische** Prozeßkonzept, das hierarchische Dateisystem mit individuellen Zugriffsrechten und der umfangreiche Werkzeugkasten. UNIX bietet eine Fülle von Entwicklungs-Programmsystemen an mit denen Programme leichter konzipiert und implementiert werden können. Die Benutzerschnittstelle besteht aus einer **Kommandosprache** (shell), mit der man wie in einer Programmiersprache Programme ausführen und miteinander verknüpfen kann. Auf PC's sind vor allem **MS-DOS** und **OS/2** verbreitet. Für viele Kleinrechnersysteme geht der Trend weg von den klassischen BS hin zu **Benutzeroberflächen** (Windows 3.11, Windows 95, Windows NT, Merlin, etc.), die an der Anwendung orientiert sind und das darunterliegende BS für den normalen Anwender **verstecken**.

Auf das BS dürfen **Schutzmaßnahmen** nicht aufgesetzt werden, sondern das BS selbst muß auf einem Kern basieren, der Schutzmaßnahmen aufbaut und geschützte Programmier- und Arbeitsumgebungen **garantiert**. Dieser Sicherheitskern ist gegen jeden **verändernden** Zugriff von außen abzusichern und er muß möglichst klein sein, damit er überschaubar bleibt und sein korrektes Verhalten mit formalen Methoden nachgewiesen werden kann. Geeignete Sicherheitsarchitekturen werden insbesondere wegen des **Datenschutzes**, **Computerviren** und der Absicherung gegen **Industriespionage** künftigen BS zugrunde liegen müssen.

Rechnertypen

Analogrechner

Die Darstellung von Werten in physikalischen Größen nennt man **analoge** Darstellung. (Spannung, Temperatur, Geschwindigkeit)

Merkmale: 1) kein Hauptspeicher, mehrere Rechenwerke
2) einfach zu programmieren
3) begrenzte Genauigkeit

Anwendungsgebiete: 1) Fertigungssteuerung
2) Kfz - Diagnose

Digitalrechner

verarbeiten numerische und alphanumerische Daten.

Merkmale: 1) genau ein Hauptspeicher und ein Rechenwerk
2) schwierig zu programmieren
3) hohe Genauigkeit

Anwendungsgebiete: 1) Bedarfsermittlung automatische Bestellung
2) Lagerhaltung
3) Bestellabwicklung
4) Kostenrechnung (Kalkulation)
5) Bildbearbeitung
6) Robotersteuerung
7) CAD, etc.

Hybridrechner

enthalten einen Analog- und Digitalteil.

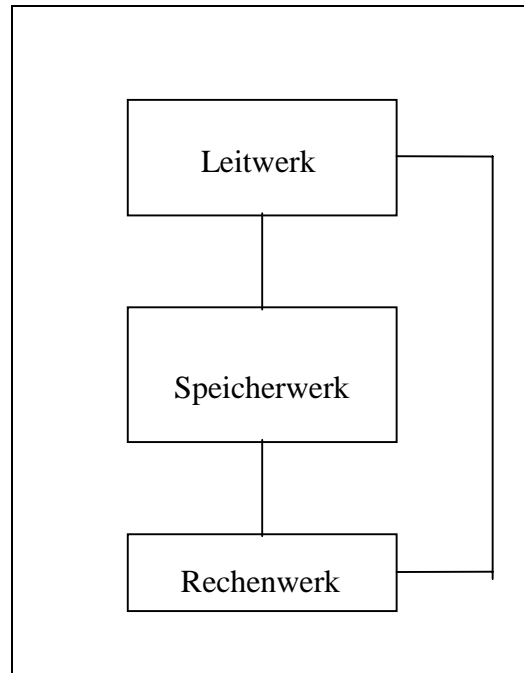
Anwendungsgebiete: 1) Prozeßsteuerung
2) Navigation
3) Chemie
4) Kraftwerke
5) NASA

Aufbau eines Computersystems

Zentraleinheit (CPU)

Eingabegeräte

Loch- oder Magnetkartenleser
Lochstreifenleser
Markierungsleser
Klarschriftleser
Handschriftleser
Meßgeräte
Signalgeber
Bildschirm mit Lichtgriffel
Tastatur
Auswahlleser
Modem



Ausgabegeräte

Lochkartenstanzer
Lochstreifenstanzer
Datensichtgerät
Sprachausgabe
Drucker
Plotter
Signalgeber
Datexleitung

Externe Speicher: Magnetplattenspeicher, Magnetbandkassetten, Magnetbänder

Leitwerk

Es koordiniert alle an der Ausführung eines Programmes beteiligten Operationen eines Computers. Die Abarbeitung der Programmbefehle werden in der gewünschten Reihenfolge gesteuert. Die Befehle werden analysiert und ausgeführt.

Der *Datenfluß* zwischen **ZE** und **Peripherie** wird gesteuert.

Folgende Schaltwerke werden dazu benötigt:

der **Taktgeber**, der die zeitliche Abfolge der einzelnen Operationen steuert

das **Befehlsregister**, ein Speicherplatz im Leitwerk, der den aktuellen Befehl enthält

der **Decodierer** für Operationsteil und Adressteil eines Befehls

der **Befehlszähler** (Adresse des nächsten Befehls)

Speicherwerk

Es ist das *Gedächtnis* des Computers (Arbeitsspeicher). Es enthält das in Arbeit befindliche Programm, die dafür benötigten Daten und vorübergehend die Ergebnisse.

Rechenwerk

Es führt die logischen und Rechenoperationen aus.

Die Ergebnisse werden im Akkumulator gespeichert

AKKU := AKKU + < 143 > ⇔ Speicher ← < Speicher > + < 143 >

Programmbefehle

Assembler	Assemblercode	Dezimal	Binär
CLC	18	24	00011000 00000000 00000000
LDA X	AD 033A	173 826	10101101 00110110 11000000
ADC Y	6D 033B	109 827	01101101 00110111 11000000
STA Z	8D 033C	141 828	10001101 00111000 11000000

Übungen

Dezimal	Fremdsystem	Dezimal	Fremdsystem
9999	10011100001111 ₂	30000	
14789	202021202 ₃	36987	
123	1323 ₄	456	
99	344 ₅	4569	
66	150 ₆	7895	
1001	2630 ₇	123580	
7892	17324 ₈	9603	
489	603 ₉	1258	
123	102 ₁₁	456	
30000	7530 ₁₆	369874125	
16414	401E ₁₆	45054	

Datensatz

Für eine Gehaltsabrechnung kann ein Datensatz wie folgt aussehen

Stellen im Datensatz (Bytes)	Inhalt
1	6 Personalnummer
7	9 Abteilung
10	15 Bruttogehalt
16	30 Bankverbindung
31	32 Steuerklasse / Religion
32	33 Kinderzahl
33	224 Monatsgehaltselement

6	Monatsgehalt brutto
5	Lohnsteuer
4	Kirchensteuer
1	Monatsschlüssel

Rechnen im Dualsystem

Addition

15	LLLL		O + O = 0
+23 (dezimal)	+LOLLL (dual)	es gilt :	L + O = L
38	LOOLLO		O + L = L
			L + L = 0 Übertrag = L

Aufgabe: 19+177+6+55=257

Subtraktion

6	OLLO		O - O = 0
-2 (dezimal)	-OOLLO (dual)	es gilt :	L - L = 0
4	OLOO		L - O = L
			O - L = L Übertrag = L

Aufgabe : 25-12=13

maschinelle Subtraktion

OLLO
+LLOL
L OOLL
+ L
OLOO

Aufgabe: 500-177-19-20=284

Multiplikation

12 · 5 = 60	LLOO · LOL
	LLOO
	OOOO
	LLOO
	LLLLOO

Aufgabe: 11 · 3 = 33

Division

6 : 2 = 3	LLO : LO = LL	$\frac{1}{3} = 0, \overline{LO}$	$\frac{1}{4} = 0, OL$
	LO		
	LO		
	LO		
	O		

Aufgaben: 35 : 5 = 7 $\frac{1}{5} =$ $\frac{1}{17} =$

Datensicherung

Aufgabe ist es den **Verlust** oder die **Verfälschung** zu verhindern.

1) technische Datensicherung

a) Speicherschutz

der Hauptspeicher wird in mehrere Bereiche aufgeteilt, wobei der Zugriff auf einen Bereich nur über eine Kennung möglich ist.

b) Paritätsprüfung

α) Querparitätsprüfung (das Byte wird geprüft)

β) Längsparitätsprüfung (der Block wird geprüft)

2) programmtechnische Datensicherung

a) Prüfziffern

die Dateneingabe von Menschen ist sehr **fehleranfällig** (8 statt 3, 34 statt 43, 3345 statt 345)

Verfahren

jede Ziffer wird mit einem Faktor multipliziert, die Produkte werden addiert und die Summe anschließend durch eine Konstante geteilt, wobei der **ganzzahlige Rest** als Prüfziffer(zahl) verwendet wird. z.B. Zahl=5749 Konstante=11 Faktoren=1, 2, 3, 4,...

$5 \cdot 1 + 7 \cdot 2 + 4 \cdot 3 + 9 \cdot 4 = 67$ $67 : 11 = 6 \text{ R } 1 \Rightarrow$ Prüfziffer(zahl) = 1

die Prüfziffer(zahl) wird der Zahl angehängt. (Kontonummern, ISBN)

b) jeder Benutzer der RA erhält einen **Code** (Stimmuster, Gestalt ,Magnetkarte, Fingerabdruck), mit dessen Hilfe er auf der Anlage arbeiten kann.

3) organisatorische Datensicherung

a) auf dem Datenträger wird vermerkt, wie oft er benutzt wurde (**Lebensdauerkontrolle**)

b) **Sicherheitskopien** werden angelegt, die **nicht** in demselben Gebäude aufbewahrt werden

c) **Archivierung** soll sicherstellen, daß alle Datenbestände jederzeit rekonstruierbar sind
drei Generationen von Bändern werden aufbewahrt

Computermisbrauchversicherung

Es wird **Schutz** vor

1) unerlaubter Benutzung der Anlage

2) unerlaubtem Zugriff auf Daten

3) Zerstörung von Programmen

4) Zerstörung von Daten

5) Totalausfall der Anlage gefordert.

Die Versicherungswirtschaft hat über die übliche Sachversicherung für DVA's eine **spezielle** Computermisbrauchversicherung entwickelt. **Fahrlässiges** Verhalten von Mitarbeitern, **vorsätzliche** Handlungen sind in der EDV besonders gefährlich.

Datenschutzgesetze

Durch sie soll der **Mißbrauch persönlicher** Daten herabgesetzt werden.

Persönliche Daten **betriebsfremder** Personen sind gespeichert bei

a) öffentliche Verwaltung

b) private Betriebe

Arbeitnehmerdaten werden gespeichert wie z.B. Leistung, Verhalten, Gesundheit, etc.
Das Datenschutzgesetz sieht vor, daß betroffene Personen **Auskunft** über ihre gespeicherten Daten bekommen und diese **eventuell** korrigiert werden.
Die **Weitergabe** von personenbezogenen Daten an **Dritte** muß geregelt sein.
(SCHUFA, Polizei, Finanzamt, Versicherungen)

Vom Problem zum Programm

- 1) Problemanalyse
- 2) Algorithmus (Lösungsverfahren) aufstellen
- 3) Programmablaufplan (PAP, flowchart) aufstellen
- 4) Programm schreiben
- 5) Programm testen
- 6) Programm verbessern, falls nötig zu 5)
- 7) Arbeitsende

Programmieraufgaben

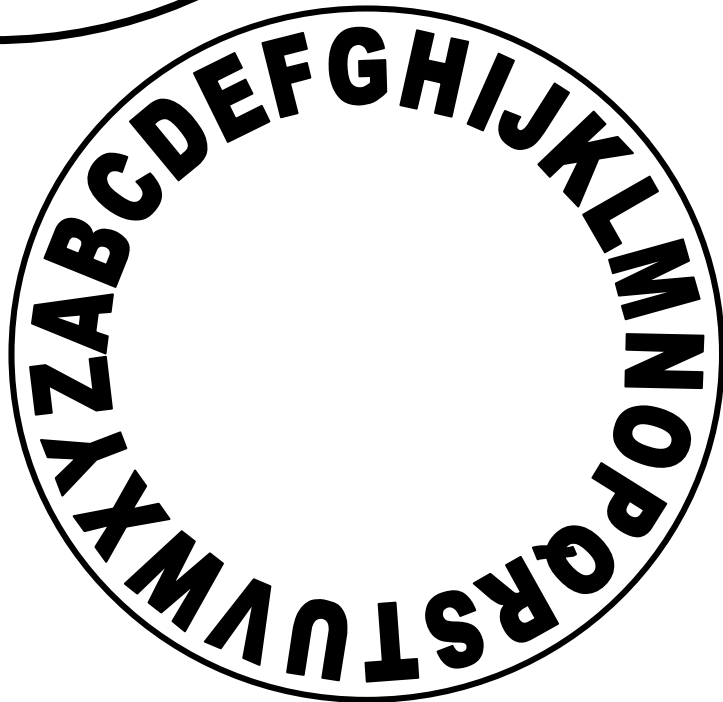
- 1) Zinsberechnung
 berechne die Laufzeit oder das Endkapital oder den Zinssatz
- 2) berechne $X=(C \cdot E - B \cdot F)/(A \cdot E - B \cdot D)$
- 3) berechne die ersten n Glieder der Fibonaccifolge
 $a_n = a_{n-1} + a_{n-2}$ $a_0 = 1$ $a_1 = 1$ $n = 2, 3, 4, \dots$
- 4) es sollen n Zahlen addiert werden, anschließend wird der Mittelwert berechnet
- 5) bestimme das Tagesdatum
 Eingabe: Tag, Monat, Jahreszahl Ausgabe: 0, 1, 2, ..., 6 wobei 0=Sonntag usw. bedeutet
 a) wenn Monat > 2, zu c)
 b) Monat := Monat + 10; Jahreszahl := Jahreszahl - 1 zu d)
 c) Monat := Monat - 2
 d) A := Jahreszahl MOD 100; C := Jahreszahl DIV 100;
 B := (13 * Monat - 1) DIV 5 + A DIV 4 + C DIV 4 W := (A + B + T - 2 * C) MOD 7
- 6) prüfe, ob eine ungerade natürliche Zahl eine Primzahl ist
 Testdaten: 43, 1807, 3263443, 257, 65537, 6700417, 30031, 209263, 25527, 2233,
 1000052561, 1000052563, 1000052567, 1000052569,
 1000105138763394623, 99999989237606677
- 7) berechne ggT(a,b) und kgV(a,b) wobei a und b natürliche Zahlen sind
- 8) eine natürliche Zahl n soll in die Dualdarstellung umgerechnet werden
- 9) die Quersumme einer natürlichen Zahl soll berechnet werden
- 10) die Prüfziffer(zahl) einer natürlichen Zahl soll berechnet werden
- 11) $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n$ einer natürlichen Zahl soll berechnet werden (n-Fakultät)
- 12) das Maximum von drei natürlichen Zahl soll berechnet werden
- 13) Text soll ver(ent)schlüsselt werden
- 14) Palindromtest Rentner, Reliefpfeiler, Reittier
 ein Neger mit Gazelle zagt im Regen nie,
 dreh Magiezettel um Amulette, zeig am Herd
 Reizherd erhitzt ihre Drehzier
 dreh mit Forelle Teller oft im Herd
 bei Liese sei lieb
 die Liebe ist Sieger, rege ist sie bei Leid
- 15) Wortratespiel (Hangman)

Anhang

Vigenèretafel

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Chiffrierscheibe für Cäsar-Verschlüsselung



Anleitung:

Beide Scheiben ausschneiden und konzentrisch aufeinander legen. Im gemeinsamen Mittelpunkt mit einer Klammer drehbar zusammenfügen.