

# **Der Informatik Spiegel**

**Dokumentation  
von Programmierarbeiten  
im  
Informatikunterricht  
an der  
Gesamtschule Gießen-Ost**



Auf den folgenden Seiten werden die im Informatikunterricht von den Schülerinnen und Schülern der Mittel- und Oberstufe der Gesamtschule Gießen-Ost erstellten Programme vorgestellt. Es handelt sich dabei um Excel-, PowerPoint- und Delphi-Programme.

Die Programme werden kurz beschrieben und eventuell gibt es auch eine Kurzanleitung zur Bedienung des Programms. Nicht zuletzt werden kurz die verwendeten Datenstrukturen, Kontrollstrukturen, Objekttypen und Algorithmen beschrieben, die bei der Programmierung verwendet wurden.

Eine Diskette mit den Programmen stellen wir jeder interessierten Schülerin und jedem interessierten Schüler gerne zur Verfügung. Ob ein Unkostenbeitrag erhoben werden muss, steht derzeit noch nicht fest.

Viel Spaß beim Lesen dieses Heftes und beim Ausprobieren der Programme!

Gießen, im März 2001

Dr. Markus Failing  
Informatiklehrer an der GGO

<b>1</b>	<b>Jahrgangsstufe 9/10</b>	<b>6</b>
1.1	Die Caesar-Verschlüsselung .....	7
<b>2</b>	<b>Jahrgangsstufe 11</b>	<b>7</b>
2.1	Rechnung .....	8
2.2	Darstellung linearer und quadratischer Funktionen .....	9
2.3	Simulation eines Kugelstoßes .....	10
2.4	Wahlanalyse .....	11
2.5	Listenverwaltung mit Excel .....	12
	<b>2.Kryptografie</b>	
2.7	Beachparty.....	13
2.8	Ernährungsratgeber .....	14
2.9	Texte invertieren und kopieren .....	14
2.10	Währungsrechner.....	15
<b>3</b>	<b>Jahrgangsstufe 12</b>	<b>16</b>
3.1	Memory .....	16
3.2	Game of Life .....	17
3.3	Der Taschenrechner .....	18
3.4	Die Türme von Hanoi.....	19
3.5	Wer wird Millionär? .....	20
3.6	Fibonacci, GGT, Potenzrechner .....	21
3.7	Rekursives Streckenzeichnen auf dem Bildschirm.....	22
3.8	Ein Sortierprogramm .....	23
3.9	Ein Suchprogramm.....	23
3.10	Formelino.....	24
3.11	PentagonHacker`s NetzPost.....	25

<b>4</b>	<b>Jahrgangsstufe 13</b>	<b>26</b>
4.1	Die Quiz-Show .....	26
4.2	Automaten und reguläre Ausdrücke.	27
<b>5</b>	<b>Programme zur Kryptographie</b>	<b>28</b>
5.1	Das Caesar-System .....	29
5.1.1	Verschlüsselung .....	29
5.1.2	Entschlüsselung .....	30
5.1.3	Brechen des Systems .....	31
5.2	Das Vigenere_System.....	31
5.2.1	Verschlüsselung .....	31
5.2.2	Entschlüsselung .....	32
5.2.3	Brechen des Systems .....	33
5.3	Das Knapsack-System .....	34
5.3.1	Produkt .....	35
5.3.2	Faktorisierung.....	35
5.3.3	Verschlüsselung .....	36

# 1 Jahrgangsstufe 9/10

Informatik im weitesten Sinne hat in der Mittelstufe der Gesamtschule Gießen-Ost bisher lediglich im Rahmen der Projektwoche im Schuljahr 2000/2001 stattgefunden. Thema war die Wissenschaft vom Verschlüsseln und Entschlüsseln von Nachrichten, Kryptografie.

Die Schülerinnen und Schüler haben mit Delphi ein Programm zur Verschlüsselung von Nachrichten geschrieben. Dabei haben alle Schülerinnen und Schüler zum ersten Mal mit Delphi programmiert.

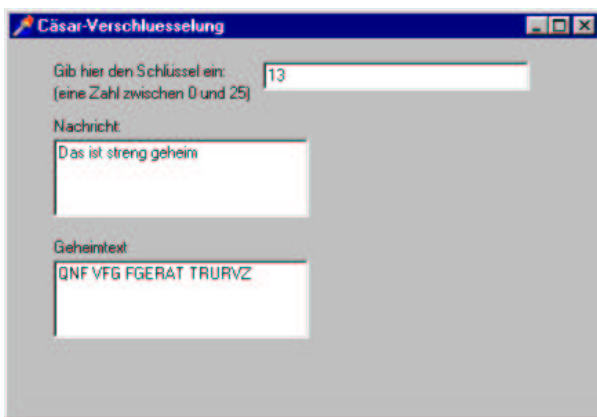
Diese Verschlüsselung basiert auf einer Methode, die Julius Caesar während seiner Kriege verwendete, um seine Nachrichten zu verschlüsseln: Jeder Nachrichtenbuchstabe wird durch den Buchstaben ersetzt, der 3 Stellen weiter im Alphabet steht, also A wird durch D ersetzt, B durch E, C durch F, ..., W durch Z, X durch A, Y durch B und Z durch A.

Man nennt die Zahl 3 den Schlüssel des Verfahrens. Dieses Caesar-Verfahren ist nicht sehr sicher, denn man kann einfach alle möglichen Schlüssel ausprobieren, es gibt ja nur 25. Es gibt noch eine weitere Methode: Der Buchstabe E ist der Buchstabe, der in deutschen Texten am häufigsten vorkommt. Das E wird aber immer durch das H ersetzt. Also müsste im Geheimtext das H am häufigsten vorkommen. So einfach ist Caesar zu entschlüsseln.

Ich wünsche mir, dass noch sehr viele solcher guter Programmierarbeiten in der Mittelstufe entstehen.

Viel Spaß mit dem Programm.

## 1.1 Die Caesar-Verschlüsselung



### Kurzbeschreibung und Kurzanleitung

Man gibt zunächst den Schlüssel, der für die Verschlüsselung verwendet werden soll, in die Edit-Komponente ein. Diese Zahl muss zwischen 0 und 25 liegen. Dabei bedeutet der Schlüssel 6, dass

alle Nachrichtentextbuchstaben um 6 Stellen im Alphabet verschoben werden. Abschließend gibt man die Nachricht ein. Der Geheimtext wird sofort Buchstabe für Buchstabe ausgegeben.

### Informatik

Neben Edit- und Labelkomponenten wird zur Berechnung der Geheimtextbuchstaben die modulare Arithmetik verwendet, also die Division mit Rest. Da die Verschlüsselung direkt nach Eingabe eines Nachrichtentextbuchstabens erfolgt, muss das Ereignis „OnChange“ der Edit-Komponente überprüft werden.

## 2 Jahrgangsstufe 11

Inhalte des Informatikunterrichts in der Jahrgangsstufe 11 sind zunächst Anwenderprogramme, also Textverarbeitung (Word), Tabellenkalkulation (Excel) und Präsentationen (PowerPoint). Dabei werden auch die Themen HTML-Programmierung und Java kurz angerissen, so dass ein grober Überblick über die wichtigsten Anwenderwerkzeuge vermittelt wird. Natürlich darf die Erforschung des Aufbaus eines PCs nicht fehlen, es geht um Datenschutz und um das Thema Computer und Gesellschaft.

Im zweiten Halbjahr der Jahrgangsstufe 11 geht es dann um das Erlernen einer objektorientierten Programmiersprache. Hier wird Delphi eingesetzt. Dieses Programm hat den Vorteil, dass bereits in sehr kurzer Zeit, meist schon in der ersten oder zweiten Unterrichtsstunde, fenstergesteuerte Programme erstellt werden können. Erste einfache theoretische Betrachtungen der Informatik werden angestellt, zum Beispiel werden die Begriffe EVA-Prinzip, Objekte, Algorithmus, Compiler, Interpreter, Struktogramme und Kontrollstrukturen erläutert.

Die hier dargestellten Programme wurden in der Regel in einem fächerverbindenden Zusammenhang erstellt, beispielsweise in Verknüpfung mit den in der Jahrgangsstufe 11 behandelten Themen der Mathematik (lineare und quadratische Funktionen), Physik (schiefer Wurf) und Wirtschafts- und Gesellschaftslehre (Wahlen). Zunächst werden die erstellten Excel-Programme, anschließend die Delphi-Projekte vorgestellt.

## 2.1 Rechnung

	A	B	C	D	E
1					
2			Pizza Panne		
3					
4		Menge	Artikel	Einzelpreis	Gesamtpreis
5		20	Pizza Einstein	9	180
6		12	Pizza Panne	12	144
7		9	Salat Tatuba	7	63
8		5	Spaghetti Cuba	10	50
9		15	Pizzabrot	4	60
10		25	Vino rosso	15	375
11		30	Vino blanco	15	450
12		24	Aqua	3	72
13				Nettopreis	1394
14				MwSt. 16%	223,04
15				Bruttopreis	1617,04

### Kurzbeschreibung und Kurzanleitung

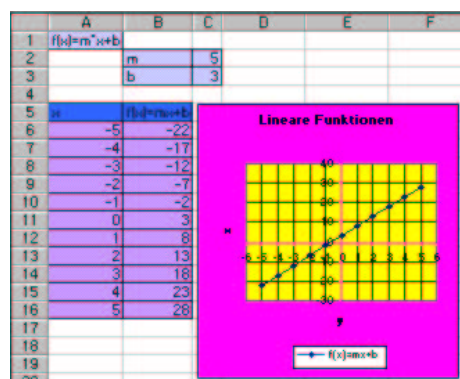
Mit diesem Programm ist es möglich, eine Rechnung für ein Abendessen professionell zu erstellen. Dabei muss nur noch die Anzahl der verspeisten Lebensmittel in der Tabelle eingegeben werden, das Programm berechnet dann die Endsumme inklusiv Mehrwertsteuer.

## Informatik

Excel ist ein Tabellenkalkulationsprogramm mit dem man zeilen- und spaltenweise Berechnungen durchführen kann. Dabei hat jede Zelle einen Namen (z.B. A5) und ist für sich ein eigener Taschenrechner. Es ist möglich, den Inhalt einer Zelle in einer anderen Zelle zu benutzen. Im Prinzip sind die Zellen auf einem Tabellenblatt wie die Zellen in einem Körper miteinander in Verbindung.

Durch die Kopierfunktion ist es möglich, eine Formel in einer Zelle auf andere Zellen zu übertragen. Ändert man nun die Anzahl der bestellten Artikel, wird in jeder Zelle mit der neuen Anzahl gerechnet. Dazu rechnet Excel mit dem Zellennamen, nicht mit dem Inhalt der Zelle.

## 2.2 Darstellung linearer und quadratischer Funktionen

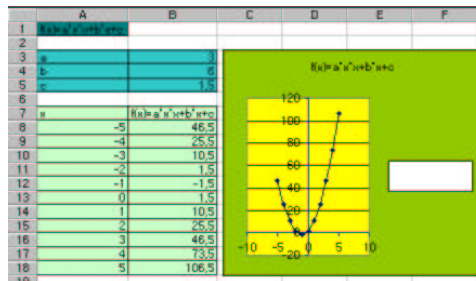


### Kurzbeschreibung und Kurzanleitung

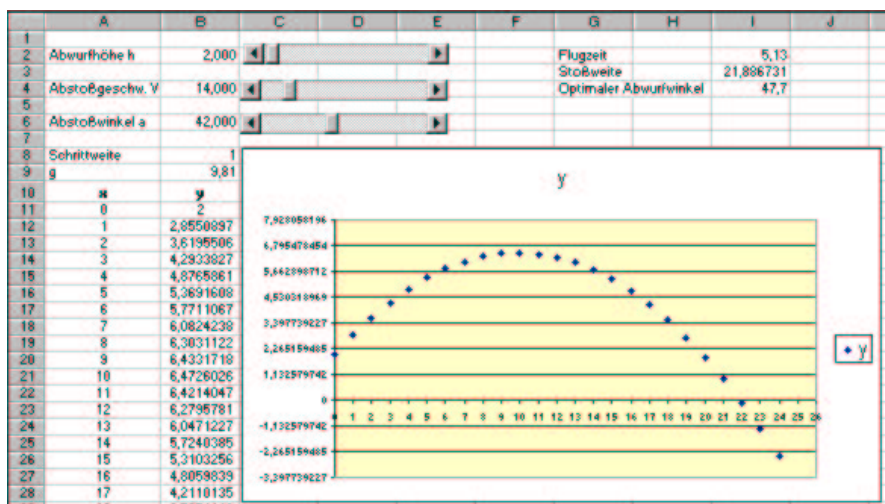
Das Programm zeichnet den Graphen linearer und quadratischer Funktionen. Eingeben muss man nur noch die Steigung  $m$  und den Achsenabschnitt  $b$  beziehungsweise die Parameter  $a$ ,  $b$  und  $c$  bei quadratischen Funktionen. Dadurch kann man einfach die Parameter abändern und das Diagramm wird automatisch mit den neuen Parametern gezeichnet.

## Informatik

In Excel gibt es den Diagrammassistenten, mit dem man sehr einfach und schnell Daten einer Tabelle grafisch darstellen kann. Die Funktionswerte in der Tabelle werden aus den Parametern  $m$ ,  $b$  beziehungsweise  $a$ ,  $b$  und  $c$  berechnet. Hier muss man mit den Zellnamen rechnen. Die neu berechneten Funktionswerte werden dann im Diagramm dargestellt.



## 2.3 Simulation eines Kugelstoßes



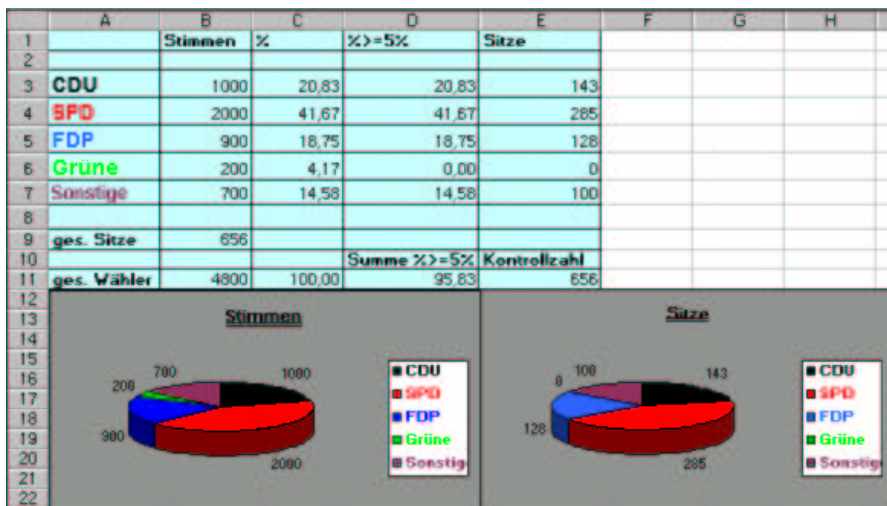
### Kurzbeschreibung und Kurzanleitung

Dieses Programm simuliert die Flugbahn eines Kugelstoßes (schiefer Wurf) und stellt sie grafisch dar. Dabei kann man die Abwurfhöhe, die Abstoßgeschwindigkeit und den Abstoßwinkel variieren. Diese können mit Scrollbalken verändert werden. Berechnet werden die Flugzeit, die Stoßweite und der optimale Abwurfwinkel.

## Informatik

Zur Änderung der Eingangswerte wurden hier Steuerelemente verwendet, die Scrollbalken. Dabei muss ein Minimalwert, ein Maximalwert, eine Schrittweite und eine Zellverknüpfung angegeben werden. Mit dem Diagrammassistenten können die in der Tabelle berechneten Werte grafisch dargestellt werden.

## 2.4 Wahlanalyse



## Kurzbeschreibung und Kurzanleitung

Dieses Programm berechnet für jede Partei die erreichten Prozente nach den erhaltenen Stimmen, überprüft, ob die 5%-Hürde geschafft wurde und teilt die zur Verfügung stehenden 656 Sitze entsprechend zu. Eine Partei erhält natürlich keine Stimme und keine Sitze, falls die 5%-Hürde nicht erreicht wurde. Die beiden Diagramme zeigen die Stimmen- und Sitzverteilung. Das Hare-Niemeyer-Verfahren regelt die Verteilung der Sitze.

## Informatik

Da in diesem Programm nur mit den Zellnamen gerechnet wird, reicht es aus, die erhaltenen Stimmen einzugeben. Die anderen Berechnun-

gen werden dann automatisch vorgenommen und auch die Diagramme werden angepasst. Neben relativen Bezügen muss hier auch mit absoluten Zellbezügen gerechnet werden, damit beim Kopieren einer Formel stets der richtige Wert der Gesamtsitze verwendet wird. Mit der Wenn-Funktion wird entschieden, ob eine Partei Sitze erhält oder nicht.

## 2.5 Listenverwaltung mit Excel

	A	B	C	D	E	F	G
1	Kundennummi	Nachnam	Vorname	Straße	Postleitzahl	Ort	Telefonnummi
2	1	Becker	Sissy	Kurt-Schumacherstr. 37	35418	Trohe	06408/7569
3	2	Berberich	Tobias	Drosselpfad 13	35428	Langgöns	06403/92141
4	3	Bolz	Anne	Alten-Buseckerstr. 9	35418	Trohe	06408/7534
5	4	Bruch	Andreas	Erentanostr.	35440	Linden	06403/71993
6	5	Eierkölle	Barbel	Torweg 11	35428	Langgöns	06403/35371
7	6	Henderson	Marius	Faltstr. 11	35440	Linden	06403/72956
8	7	Hofmann	Denise	Ernst-Ludwigstr. 5	35418	Buseck	06408/4155
9	8	Horn	Halina	Ulmenring 55	35418	Buseck	06408/4466
10	9	Kern	Jan	Bullerbüweg 32	35440	Linden	06403/5814
11	10	Klos	Marco	Schützenweg 100	35418	Buseck	06408/940816
12	11	Körber	Michael	Kiesweg 12	35396	Wiebeck	0641/51585
13	12	Landgraf	Kolja	Moltkestraße 11	35440	Linden	06403/2656
14	13	Mank	Nils	Schustergrasse 1	35396	Wiebeck	0641/5599328
15	14	Mellor	Carina	Schützenweg 42	35418	Buseck	06408/3641
16	15	Müller	Stephan	Gr. Steinweg 4	35390	Gießen	0641/34367
17	16	Pinz	Fabian	Fasanenweg 54	35396	Wiebeck	0641/53090
18	17	Schwalb	Marius	Bergstr. 45	35418	Buseck	06408/3518
19	18	Staudte	Franziska	Bismarckstr. 12	35418	Buseck	06408/3982
20	19	Wagner	Marco	Zellstr. 39	35418	Buseck	06408/5358
21	20	Wagner	Norman	Ulanstr. 45	35398	Rödgen	0641/45237
22	21	Zeller	Julian	Schillerstr. 52	35440	Linden	06403/5841

### Kurzbeschreibung und Kurzanleitung

Mit diesem Programm kann man seine eigene Telefonliste anlegen und verwalten. Ist man auf der Suche nach einer Telefonnummer, kennt aber nur noch beispielsweise den Vornamen „Martin“ des gesuchten Telefonpartners, so kann man einfach mit einem Filter alle „Martins“ herausfiltern. Dabei sucht Excel nach Eingabe eines Vornamens oder eines Nachnamens oder einer Straße alle passenden Einträge heraus.

### Informatik

Mit dem Autofilter ist es möglich, nach einzelnen Daten in einer Liste zu suchen. Mit Hilfe einer Maske kann dann noch ein Datensatz bearbeitet, hinzugefügt, gesucht oder gelöscht werden. Eine Möglichkeit, die Liste zu sortieren besteht auch: Einfach den Sortierbutton klicken

und schon ist die Liste aufsteigend oder absteigend sortiert. Mit einem Spezialfilter lassen sich weitere Datensätze herausfiltern.

## 2.6 Athen

„Athen“ ist eine PowerPoint-Präsentation, die die Klasseneinteilung in Athen um 594 v. Chr. erklärt.



## 2.7 Beachparty



„Beachparty“ ist ebenfalls eine PowerPoint-Präsentation, die in einem zweistündigen Exkurs in die PowerPointwelt erstellt wurde.

## 2.8 Ernährungsratgeber

### Kurzbeschreibung und Kurzanleitung

Mit diesem Programm kann man ermitteln, ob man Über-, Normal- oder Untergewicht hat. Dies wird aufgrund des Taillenumfangs berechnet. Nach Eingabe des Umfangs legt man noch

fest, ob die Diagnose für eine Frau oder einen Mann erstellt werden soll und klickt auf den „Berechnen“-Button. Anschließend erscheint der Ernährungsrat.

### Informatik

Verwendet werden die Objekte Radiogroup, Button und Edit-Komponenten, wobei durch mehrfach ineinandergeschachtelte If-Then-Else-Anweisungen der Ratschlag ermittelt wird. Prinzipiell könnte man auch eine Case-Struktur verwenden.

## 2.9 Texte invertieren und kopieren

### Kurzbeschreibung und Kurzanleitung

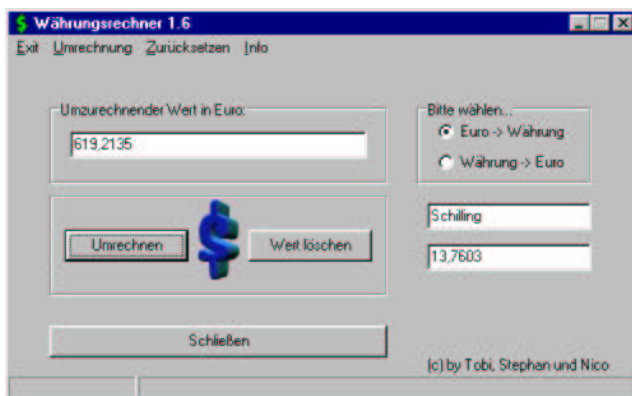
Nach Eingabe eines Textes werden die Buchstaben in umgekehrter Reihenfolge wieder ausgegeben oder kopiert. Mit dem „Neu“-Button wird die Eingabe und die Ausgabe wieder ge-

löscht, der „Exit“-Button beendet das Programm.

### Informatik

Bei diesem Programm wird zunächst die Länge des eingegebenen Wortes ermittelt. Dafür gibt es eine Funktion „Length“. Anschließend wird in einer for-Schleife von der Länge des Wortes bis runter zur „Eins“ die Buchstaben des eingegebenen Wortes ermittelt und in der zweiten Edit-Komponente ausgegeben.

## 2.10 Währungsrechner



### Kurzbeschreibung und Kurzanleitung

Mit Hilfe dieses Programms können sämtliche europäische Währungen in Euro umgerechnet werden. Dabei wird der Umrechnungs-

kurs angezeigt. Mit dem „Umrechnen“-Button wird die Umrechnung gestartet. Fährt man mit der Maus über die Buttons und Edit-Komponenten, erscheint unten ein Hilfetext.

### Informatik

Neben einer menügesteuerten Ein- und Ausgabe wurden hier Edit-komponenten, Buttons und Radiogroups als Objekte verwendet. Weiterhin wurde eine „if-then-else“-Kontrollstruktur verwendet, um die Richtung der Umrechnung zu entscheiden. Zusätzlich wurde ein Bild (Dollarzeichen) auf dem Formular eingebunden, welches nach Klicken des „Umrechnen“-Buttons die Farbe wechselt.

## 3 Jahrgangsstufe 12

Inhalte des Informatikunterrichts in der Jahrgangsstufe 12 sind höhere Datenstrukturen (Listen, Stapel, Binärbäume) und das systematische Problemlösen mit dem Computer (rekursive und iterative Verfahren). Dies ist weitgehend unabhängig von einer bestimmten Programmiersprache, so dass Schülerinnen und Schüler hier auch in Visual Basic, Java oder Delphi programmieren können, je nach Geschmack.

Anhand von ausgeklügelten Algorithmen werden Sortier- und Suchverfahren diskutiert. Ein wichtiger Unterrichtsinhalt sind so genannte Zeiger, mit denen Speicherplätze zur Laufzeit der Programme belegt werden. Dies hat große Vorteile gegenüber einer statischen Speicherplatzverwaltung.

Im Rahmen eines größeren Projektes, dessen Thema sich die Schülerinnen und Schüler frei wählen konnten, sind die folgenden hervorragenden Programmierarbeiten entstanden. Einzige Richtlinie war, die bisher gelernten Strukturen weitgehendst zu verwenden. So bauen die meisten Programme auf Arrays auf, einige enthalten interaktive und rekursive Algorithmen zur Berechnung eines Ergebnisses.

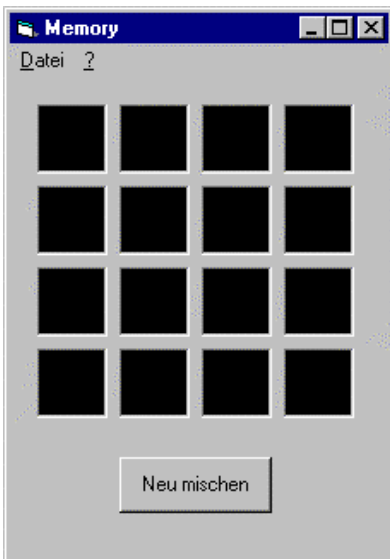
Obwohl die grafische Realisierung der Themen im Informatikunterricht nicht die vordergründige Rolle spielt, ist es den Schülerinnen und Schülern sehr gut gelungen, ihre Programme optisch aufzuwerten.

### 3.1 Memory

#### **Kurzbeschreibung und Kurzanleitung**

Memory ist ein Spiel, das ihre Konzentration fordert. Ziel ist es, Karten gleicher Farbe zu finden, indem man die schwarzen Karten aufdeckt. Hat man ein gleiches Paar entdeckt, so bleibt es offen.

Durch geschicktes Kombinieren und der Verwendung der Maus können Sie es schaffen, alle Pärchen innerhalb kürzester Zeit zu entschlüsseln.



### Informatik

Neben den kleinen Gimmicks der Soundwiedergabe mit Hilfe des Multimedia-Players haben wir für die Felder ein 16 dimensionales Array verwendet. Sortiert wird nach dem Setzkastensystem (Mischung der Karten). Ansonsten haben wir If-Anweisungen zum Vergleichen der Felder, For-Next Schleifen zum Einfügen von Pausen und verschiedene andere Kontrollstrukturen verwendet.

© 2001 Markus Blümchen und Andreas Maus

## 3.2 Game of Life

### Kurzbeschreibung

Das Programm simuliert eine Zellkultur. Die einzelnen Zellen gehorchen genauen festgelegten Regeln. Die Zellkultur besteht aus einem beliebig großen Raster. Jede Zelle hat 8 Nachbarn. In jedem Schritt werden die sterbenden und lebenden Zellen neu berechnet. Dabei wird folgende Regel angewendet: Tod durch Vereinsamung, wenn eine Zelle weniger als 2 lebende Nachbarn hat. Tod durch Überbevölkerung, wenn eine Zelle mehr als 3 lebende Nachbarn hat. Geburt einer Zelle bei genau 3 lebenden Nachbarn. Am Anfang setzt man ein Muster aus Zellen und kann sich die Simulation anschauen.



### Kurzanleitung

Nach dem Starten des Programms kann man mit der linken Maustaste ein Muster bestimmen. Mit der rechten Maustaste kommt man in ein Menü, indem man die Simulation starten, stoppen und weitere Optionen ausführen kann. Im Optionsmenü kann man die Größe des Spielfeldes und die Geschwindigkeit der Lebenszyklen festlegen.

### Informatik

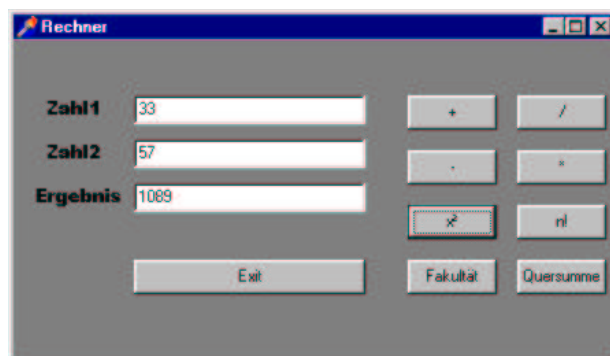
Die Zellkultur wird durch ein Array aus Boolean-Variablen dargestellt. True steht für eine lebende Zelle und False für eine tote Zelle. Bei jedem Lebenszyklus werden von jeder Zelle die lebenden Nachbarn gezählt. Dann werden auf jede Zelle die geltenden Regeln angewandt und die entstandenen Zellen in einem zweiten Array gespeichert. Am Ende wird das zweite Array wieder in das erste Array geschrieben und gezeichnet.

© 2001 Anselm Föhr und Niklas Mohr

## 3.3 Der Taschenrechner

### Kurzbeschreibung

Unser Taschenrechner verfügt über die Grundfunktionen der Mathematik. Wir haben acht Rechenfunktionen, die über Buttons aufgerufen werden: Addition, Subtraktion, Multiplikation, Division, zwei Fakultäten, Quadratzahl und Quersumme. Über den Button „Exit“ verlässt man das Programm.



### Kurzanleitung

Es gibt zwei Felder, mit „Zahl 1“ und „Zahl 2“ betitelt. Dort werden die zu berechneten Zahlen eingetragen. Will man z.B. zwei Zahlen voneinander subtrahieren, werden beide Zahlen in die Felder eingetra-

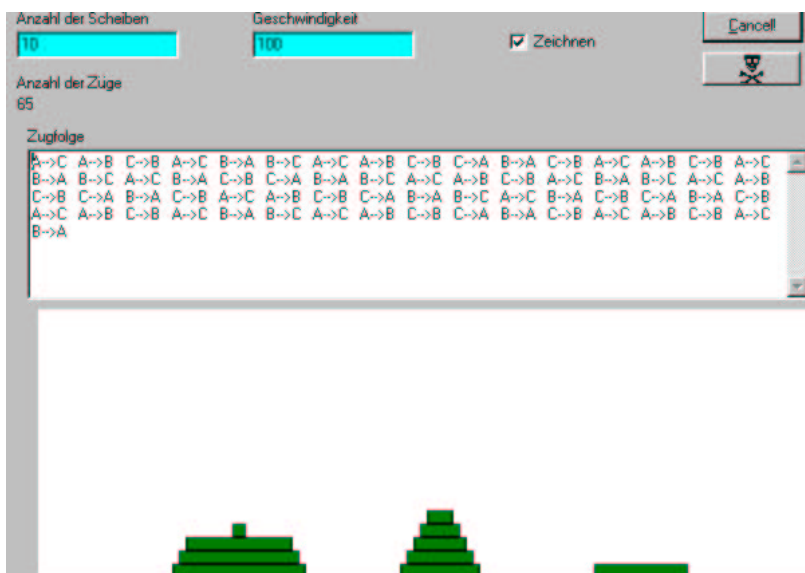
gen, danach wird der entsprechende Button gedrückt, ebenso bei +, \* und /. Bei allen anderen Funktionen wird die Zahl in das erste Feld eingetragen und die Funktion ausgeführt. Im Ergebnisfeld erscheint auch Selbiges.

### Informatik

Bei +,-,/,und \* sehen die Prozeduren alle ähnlich aus. Zahl 1 und Zahl 2 werden vom Datentyp „String“ in den Datentyp „Float“ umgewandelt. Dann erfolgt der Rechengvorgang, nach Umwandlung von Float nach String wird das Ergebnis ausgegeben. Bei der Division ist mit einer if-then-else Anweisung eine Prozedur eingebaut, die dem Benutzer mitteilt, das der Rechner nicht durch Null dividieren kann. Die Quadratzahlanweisung wird genauso ausgeführt wie die Multiplikation, mit dem Unterschied, dass die Zahl 1 mit sich selbst multipliziert wird. Bei der n!- und der Quersummen-Funktion haben wir eine Prozedur mit einer For-Schleife und eine Funktion mit einer if-then-else Anweisung verwendet.

© 2001 Julian Wessel & Sascha Loubal

## 3.4 Die Türme von Hanoi



### Kurzbeschreibung

Das Programm berechnet einen Lösungsweg vom Spiel „die Türme von Hanoi“ mit einer beliebigen Turmhöhe. Dabei können die einzelnen Rechenschritte grafisch ausgegeben werden.

Das Spiel läuft folgendermaßen ab: Es gibt drei Plätze auf denen eine beliebige Anzahl an Scheiben liegen darf. Es ist zu beachten, dass niemals eine größere auf einer kleineren Scheibe liegen darf. Ziel ist es den Turm zu verschieben. Man darf jedoch immer nur eine Scheibe bewegen.

### Kurzanleitung

Man gibt die Anzahl der Scheiben und die Geschwindigkeit ein und drückt auf „Start“.

Viel Spaß beim Zuschauen!

### Informatik

Der Lösungsweg wird mit einer rekursiven Funktion berechnet. Hierbei wird das Problem, einen großen Turm von A nach B zu bewegen zerlegt in die Probleme: 1. Einen kleineren Turm von A nach C zu bewegen und 2. die übrig gebliebene Scheibe von A nach B zu bewegen und schließlich 3. den kleineren Turm von C wieder auf B zu bewegen.

© 2001 Anselm Föhr und Niklas Mohr

## 3.5 Wer wird Millionär?

### Kurzbeschreibung und Kurzanleitung

Dieses Programm ist ein Spiel zu der bekannten und beliebten TV-Show „Wer wird Millionär?“ mit Günter Jauch. Entsprechend ihrer Gewinnchancen wird eine Frage mit einem bestimmten Schwierigkeitsgrad eingeblendet, die Sie

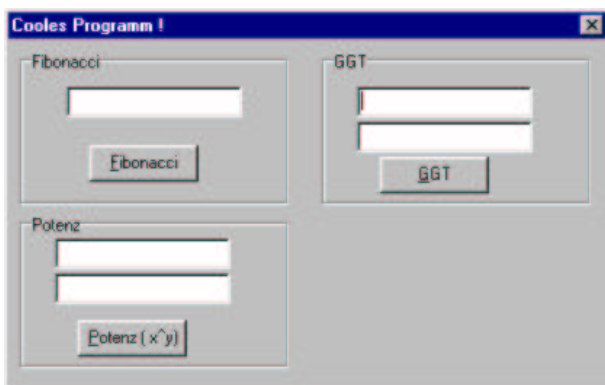


durch Drücken des Antwort-Button beantworten können. Aber nehmen Sie sich in Acht: Falls Sie eine Frage falsch beantworten, könnte schlimmes mit Ihrem Computer geschehen...

### Informatik

Zur Speicherung der Fragen wird ein dreidimensionaler Array verwendet. Die erste Dimension speichert die Fragen (von der 100 DM Frage bis zur 1000000 DM Frage), die zweite die Antworten und die dritte ist zur Speicherung verschiedener 100 DM bis 1 Mio. DM Fragen reserviert. Durch einen Zufallsgenerator wird eine entsprechende Frage ausgewählt und erscheint dann in der Edit-Komponente. Mittels einer Case-Abfrage wird der Geldbetrag bei richtiger Beantwortung erhöht. Durch if-then-else Anweisungen wird überprüft, ob der richtige Button gedrückt wurde.

## 3.6 Fibonacci, GGT, Potenzrechner



### Kurzbeschreibung

Dieser Rechner berechnet die Fibonacci-Zahlen, den größten gemeinsamen Teiler zweier Zahlen und die Potenz zweier Zahlen.

### Kurzanleitung

Zur Berechnung werden einfach die Zahl(en) in die entsprechenden Edit-Komponenten eingegeben und der entsprechende Button gedrückt.

### Informatik

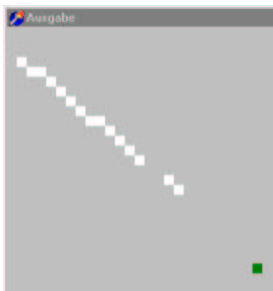
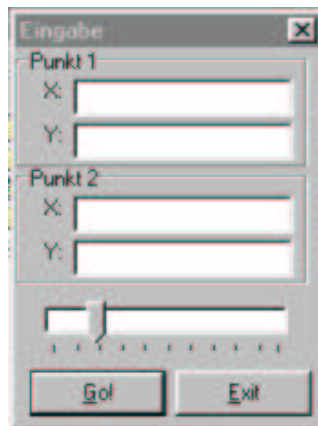
Eine Fibonacci-Zahl ist die Summe der beiden vorherigen Fibonacci-Zahlen. Dabei ist die erste Fibonacci-Zahl gleich Null, die zweite gleich 1. Die Folge lautet also 0, 1, 2, 3, 5, 8, 11, ... Die Fibonacci-

Zahl wird hier durch einen rekursiven Algorithmus berechnet, ebenso die Potenz und der GGT zweier Zahlen.

### 3.7 Rekursives Streckenzeichnen auf dem Bildschirm

#### Kurzbeschreibung und Kurzanleitung

Dieses Programm zeichnet eine gerade Linie auf den Bildschirm. Dabei gibt man die x- und y-Komponente des ersten und zweiten Punktes in die Edit-Komponenten ein. Mit dem Button „Go“ wird die Berechnung ausgeführt.

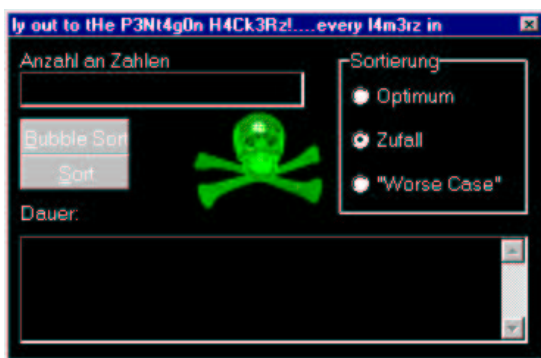


#### Informatik

Der Algorithmus zum rekursiven Streckenzeichnen geht so: Das Programm ermittelt den Mittelpunkt zwischen den beiden zu verbindenden Punkten. Nun wird zunächst die erste „Halbstrecke“ anschließend die zweite „Halbstrecke“ gezeichnet. Zum Zeichnen der ersten „Halbstrecke“ wird diese erneut zerlegt, also zunächst der Mittelpunkt berechnet und dann die entsprechenden „Halbstrecken“ gezeichnet.

Es wird allerdings erst dann ein Punkt farbig markiert, wenn der Mittelpunkt direkt neben einem der zu verbindenden Punkte liegt. Klar ist, dass dieser Algorithmus sehr langsam ist und so nicht zum Streckenzeichnen auf dem Bildschirm verwendet wird. Allerdings kann man sehr schön die Idee der Rekursion direkt am Bildschirm verfolgen, da sich die Strecke aus vielen Teilstrecken zusammensetzt, die in der Regel nicht fortlaufend gezeichnet werden.

### 3.8 Ein Sortierprogramm



#### Kurzbeschreibung und Kurzanleitung

Dieses Programm sortiert eine Anzahl von Zahlen in aufsteigender Reihenfolge. Die Sortierung kann für ein bereits sortiertes Feld (Optimum), ein zufällig generiertes Feld (Zufall) oder für ein umgekehrt sortiertes Feld (Worse Case) erfolgen. Ziel ist es zu ermitteln, welcher Algorithmus das Feld am schnellsten sortiert und wie lange er dafür benötigt.

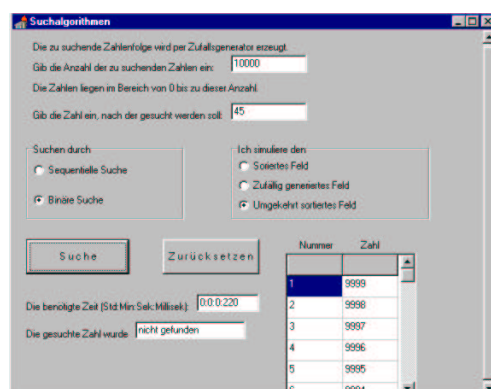
#### Informatik

Realisiert sind zwei Sortieralgorithmen, deren Effizienz und Speicherplatzbedarf verglichen werden. Als Datenstruktur dient ein Array, in dem die zu sortierenden Zahlen gespeichert werden. Effizienzbetrachtungen sind in der Regel sehr schwierig durchzuführen. Es gilt aber: Je schneller der Algorithmus, desto mehr Speicherplatz wird benötigt und umgekehrt.

### 3.9 Ein Suchprogramm

#### Kurzbeschreibung und Kurzanleitung

Mit diesem Programm kann eine Zahl unter 250000 Zahlen gesucht werden. Man gibt die Anzahl der Zahlen ein und die Zahl, nach der gesucht werden soll. Anschließend wählt man noch den

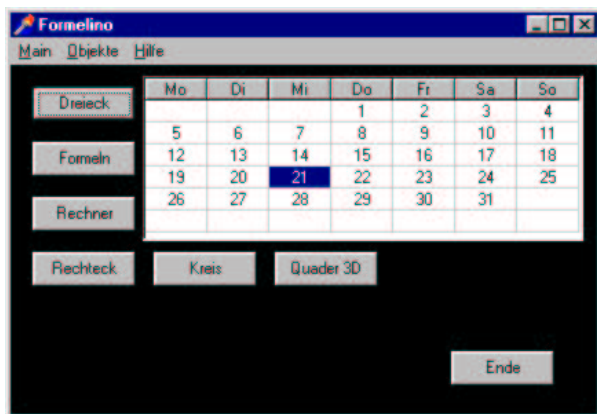


Suchalgorithmus aus und ob ein bereits sortiertes Feld, ein zufällig generiertes Feld oder ein umgekehrt sortiertes Feld vorliegen soll. Ausgegeben wird die für die Suche benötigte Zeit und an welcher Stelle die Zahl gefunden wurde.

### Informatik

In Arrays werden die Zahlen zunächst gespeichert. Per Zufallsgenerator werden die Zahlen erzeugt und in der gewünschten Reihenfolge gespeichert. Implementiert sind zwei verschiedene Suchalgorithmen: Interessant ist die binäre Suche, in der das sortierte Feld jeweils in zwei Hälften zerlegt wird und anschließend in den beiden Hälften genau so vorgegangen wird. Die „einfache“ sequentielle Suche, bei der einfach „vorn“ begonnen wird und alle Zahlen durchlaufen werden ist der zweite Algorithmus, mit dem nach einer Zahl gesucht werden kann. Durch Effizienzvergleiche kann so der „beste“ Algorithmus ermittelt werden.

### 3.10 Formelino



#### Kurzbeschreibung und Kurzanleitung

Das Programm kann sämtliche Eigenschaften von Rechtecken, Kreisen, Dreiecken oder Quadern berechnen. Des Weiteren enthält das Programm einen Taschenrechner, einen Kalender und

eine Formelsammlung für Physik und Mathe. Um zu dem Fenster mit Rechteck zu gelangen, muss man nur auf den Button mit der Aufschrift „Rechteck“ klicken und das Fenster wird geöffnet. Wenn Sie ein Fenster geöffnet haben, können Sie in den dafür vorgesehenen

Feldern z.B. a; b einen Wert eintragen und auf z.B. den Button mit der Aufschrift „Umfang“ klicken und der Umfang erscheint im Ausgabefeld.

### **Informatik**

In dem Programm wurden edit- Komponenten und Buttons verwendet. Das Programm arbeitet hauptsächlich mit der Kontrollstruktur „if-else“. Weiterhin wurde „case“ , „Speichermodule“ , Radiogroups und einzelne Funktionen, wie „Pi“ und „sqrt“ (Wurzel) verwendet.

© 2001 Jens Türschmann und Philipp Rodrique

## **3.11 Pentagon-Hacker`s NetzPost**

### **Kurzbeschreibung und Kurzanleitung**

Dieses Programm ermöglicht die Kommunikation zwischen Lehrer und Schülern via PC im TCP/IP Netzwerk. Es steigert die Effizienz der Lerngruppe, durch die Möglichkeit mehrere Dialoge gleichzeitig zu führen, wobei jeder Einzelne vom Lehrer überwacht werden kann und dieser Kommentare einfließen lassen kann. Dadurch werden Diskussionsdauer und Wartezeiten für unbeteiligte Schüler um ein vielfaches verkürzt. Mit NetzPost können Argumente, Fragen, Antworten usw. an beliebig viele Mitschüler versendet werden, ohne dass arbeitende Schüler durch Lärm belästigt oder gestört werden. Ein weiterer positiver Nebeneffekt ist sicherlich die Förderung der Schüler im Umgang mit dem PC, der in Zukunft unerlässlich sein wird, da er ein großen Teil unsere Arbeit übernehmen wird .

Die Oberfläche von NetzPost wurde bewusst einfach strukturiert. Die Bedienung ist denkbar einfach:

Der gewünschte Text wird in das untere Feld eingegeben. Anschließend wählen Sie die Adressaten und schicken ihre Nachricht ab. Wie im richtigen Leben. Das Ganze ist natürlich umsonst, geht schneller und sicherer als jeder Brief.

## 4 Jahrgangsstufe 13

Hauptinhalt der Jahrgangsstufe 13 ist die Automatentheorie. Es werden endliche Automaten betrachtet und durch verschiedene Darstellungsformen beschrieben (reguläre Ausdrücke, reguläre, kontextfreie und kontextsensitive Sprachen und Typen und Grammatiken formaler Sprachen werden betrachtet. Hinzu kommen Ein- und Zweikellerautomaten und schließlich der Turingautomat. Hauptfragen sind:

- was ist berechenbar und entscheidbar?
- welche prinzipiellen Grenzen algorithmischer Verfahren gibt es?
- wie funktioniert ein Compiler?
- wo sind die Grenzen formaler Kommunikation?

Als zweites großes Thema wurde bisher die künstliche Intelligenz betrachtet. Anhand eines Kommunikationsprogrammes (ELIZA) werden Techniken der KI ergründet und getestet. Themen der neuronalen KI schließen sich an.

Das Thema eines größeren Projektes wird in der Regel freigestellt. Hier ist Raum für die Erstellung einer Homepage (HTML-Programmierung) oder Arbeiten mit dem Programm „Flash“ (Erstellung von animierten Sequenzen).

### 4.1 Die Quiz-Show

#### Kurzbeschreibung und Kurzanleitung

Das Programm muss lediglich gestartet werden. Anschließend erscheint der Moderator und stellt seine Fragen. In einem Kreis läuft die Zeit von 30 Sekunden ab. Klickt man auf die richtige Antwort, erscheint die nächste Frage. Ansonsten startet

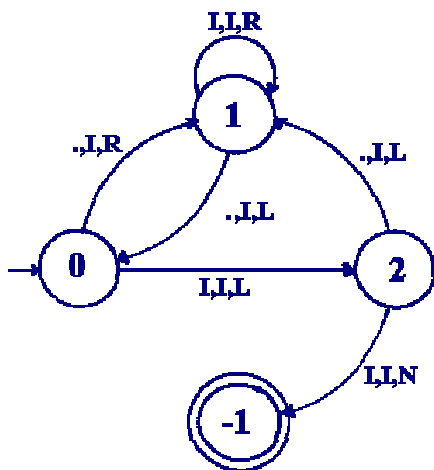


das Programm neu.

### Informatik

Das Programm wurde mit „Flash“ geschrieben. Dieses Programm ermöglicht es, verschiedene Filmsequenzen übereinander zu legen. Man definiert ein erstes Bild und das Schlussbild, den Übergang von Startbild zum Schlussbild berechnet „Flash“ selbst. „Flash“ ist die Grundlage vieler kommerzieller Adventurespiele. Als Projekt fand es im Informatikunterricht großen Anklang bei den Schülern.

## 4.2 Automaten und reguläre Ausdrücke



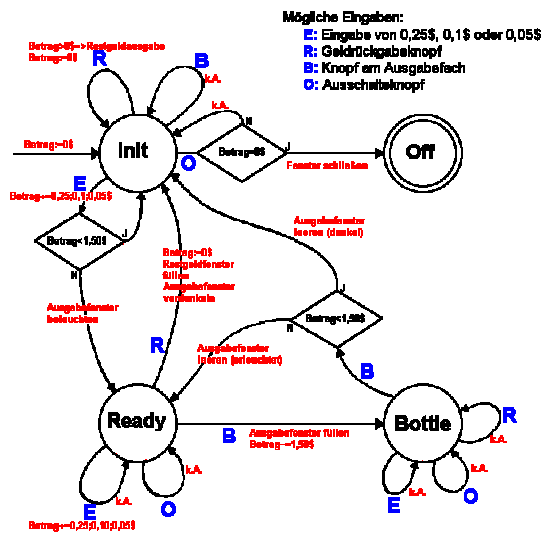
### Informatik

Die nebenstehende Abbildung zeigt einen so genannten Zustandsgraphen eines Automaten. Dies ist eine Möglichkeit von vielen, Automaten darzustellen.

In der nachfolgenden Abbildung wird ein Getränkeautomat dargestellt. Die Knoten stellen die verschiedenen Zustände des Automaten dar (z.B. „Bottle“

kennzeichnet den Auswurf der Flasche), durch die Pfeile werden die Eingaben (z.B. 1 DM, 2 DM, ...) dargestellt. In Abhängigkeit der verschiedenen Eingaben bleibt der Automat im alten Zustand oder gelangt in einen neuen Zustand. Als Erweiterung wird in Abhängigkeit des Zustandes und der Eingabe eine Ausgabe ermittelt (z.B. die Meldung, dass 1,50 DM eingeworfen wurden).

Die Programmierung des Automaten ist noch in Arbeit.



## 5 Programme zur Kryptografie

Auf den folgenden Seiten möchte ich die von mir erstellten Programme zur Kryptografie kurz vorstellen, die mehrfach in meinem Unterricht Anwendung gefunden haben.

Es handelt sich dabei um das symmetrische, monoalphabetische Caesar-Verfahren und das symmetrische, polyalphabetische Vigenere-Verfahren.

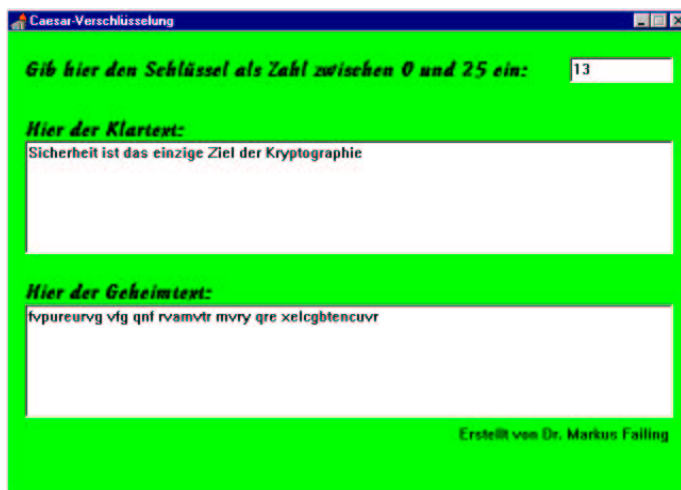
Außerdem habe ich ein Knapsackverfahren umgesetzt, welches ein Beispiel für ein unbrechbares, asymmetrisches Verfahren darstellt. Um dieses System zu brechen, würde man PCs mit einem Arbeitsspeicher benötigen, der der Masse des Universums entspricht und eine Zeit in der Größenordnung des Alters des Universums. Kurzum: Mit „normalen“ Mitteln ist dieses System nicht zu brechen. Aber: Es gibt ja noch die Mathematik. Bereits seit längerer Zeit ist ein mathematisches Hintertürchen bekannt, mit dem das System zu brechen ist. Fa-

zit: Was nützen die schnellsten PCs, wenn es mit guter Mathematik dann doch zu brechen ist? Was bedeutet also Sicherheit einer Nachricht?

Zurzeit arbeiten die besten Mathematiker und Informatiker an einem unbrechbaren System, immer wieder tauchen Nachrichten im Internet auf, ein solches System sei gefunden. Zurzeit bieten die asymmetrischen Verfahren den besten Schutz vor einem Angriff, bis die Mathematik erneut ein Hintertürchen findet ....

## 5.1 Das Caesar-System

### 5.1.1 Verschlüsselung



Zunächst muss der Schlüssel für die Verschlüsselung eingegeben werden. Anschließend wird jeder Nachrichtentextbuchstabe sofort bei der Eingabe verschlüsselt und in der Geheimtext-Edit-

Komponente ausgegeben.

Bei der Verschlüsselung wird jeder Buchstabe durch denjenigen Buchstaben ersetzt, der im Alphabet um so viel Stellen weiter steht, wie der Schlüssel angibt.

Beispiel: A wird mit dem Schlüssel 2 zu C.

Bei der Programmierung werden die Buchstaben zunächst durch Zahlen ersetzt:

A entspricht 0, B entspricht 1, ..., Z entspricht 25. Dann wird der Geheimtextbuchstabe berechnet.

Beispiel: A entspricht 0, Schlüssel = 2: Geheimtextbuchstabe entspricht  $0+2=2$ , also C.

### 5.1.2 Entschlüsselung

Zunächst muss der Schlüssel für die Entschlüsselung eingegeben werden. Anschließend wird jeder Geheimtextbuchstabe sofort bei der Eingabe entschlüsselt und in der Nachrichtentext-Edit-



Komponente ausgegeben.

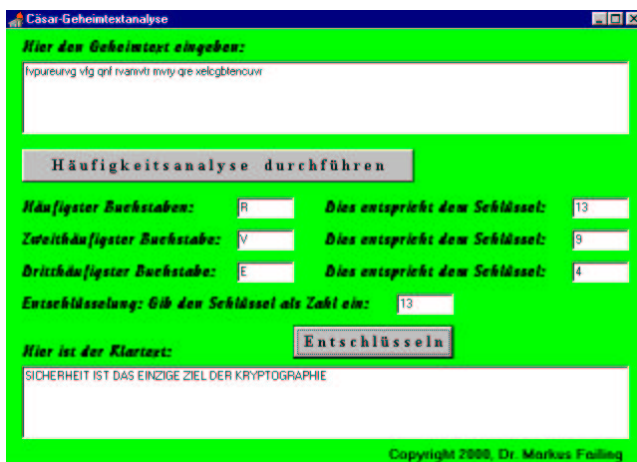
Bei der Entschlüsselung wird jeder Buchstabe durch denjenigen Buchstaben ersetzt, der im Alphabet um so viel Stellen vorher steht, wie der Schlüssel angibt.

Beispiel: C wird mit dem Schlüssel 2 zu A.

Bei der Programmierung werden die Buchstaben zunächst durch Zahlen ersetzt: A entspricht 0, B entspricht 1, ..., Z entspricht 25. Dann wird der Geheimtextbuchstabe berechnet.

Beispiel: C entspricht 2, Schlüssel = 2: Geheimtextbuchstabe entspricht  $2-2=0$ , also A.

### 5.1.3 Brechen des Systems



Das Caesar-System ist einfach zu brechen: In deutschen Texten ist E der häufigste Buchstabe. Da jeder Nachrichtentextbuchstabe stets durch denselben Geheimtextbuchstaben ersetzt wird, überträgt

sich die Häufigkeit der Buchstaben im Nachrichtentext auf die Buchstaben im Geheimtext. Um das System zu knacken, muss der Schlüssel ermittelt werden. Ist beispielsweise G der häufigste Buchstabe im Geheimtext, so kann man annehmen, das G dem E im Nachrichtentext entspricht. Das heißt, der Schlüssel wäre 2.

Das Programm führt nach Eingabe des Geheimtextes eine Buchstabenhäufigkeitsanalyse durch und zeigt die drei häufigsten Buchstaben an. Danach gibt man den vermuteten Schlüssel ein und der Nachrichtentext wird ausgegeben.

## 5.2 Das Vigenere-System

### 5.2.1 Verschlüsselung

Das Vigenere-System ist ein polyalphabetisches System. Während beim Caesar-System stets nur ein Schlüssel/Buchstabe zur Verschlüsselung verwendet wird, benutzt man beim Vigenere-System mehrere Schlüssel, ein Schlüsselwort.

Beispiel: Schlüsselwort sei ICH, dies entspricht den Schlüsseln 8, 2, 7.  
 Die Nachricht sei GUT. Dies entspricht 6, 20, 19. Der Geheimtext ist nun  
 $8 + 6 = 14$ , entspricht O.  
 $2 + 20 = 22$ , entspricht W.  
 $7 + 19 = 26$ , entspricht A.  
 Der Geheimtext lautet: OWA.

Der Vorteil gegenüber dem Caesar-System besteht in der Verschleierung der Häufigkeiten der Buchstaben, denn ein Buchstabe kann nun durch verschiedene Buchstaben ersetzt werden.



## 5.2.2 Entschlüsselung



Die Entschlüsselung verläuft analog zur Verschlüsselung:

Beispiel: Schlüsselwort sei ICH, dies entspricht den Schlüsseln 8, 2, 7. Der Geheimtext sei OWA. Dies entspricht 14, 22, 26. Der Nachrichtentext

ist nun

$14 - 8 = 6$ , entspricht G.

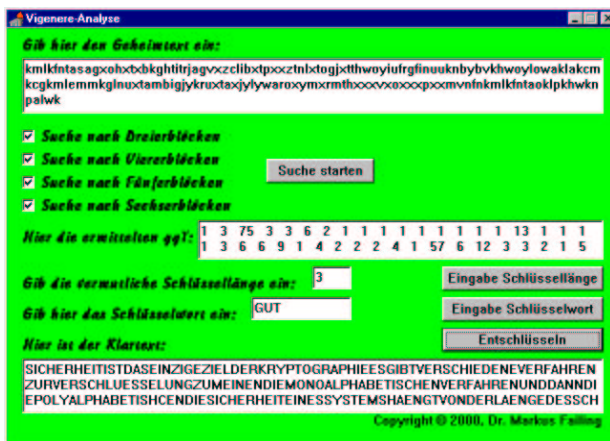
$22 - 2 = 20$ , entspricht U.

$26 - 7 = 19$ , entspricht T.

Der Nachrichtentext lautet: GUT.

Sollte die Subtraktion ein negatives Ergebnis liefern, so muss 26 hinzuaddiert werden, um den Nachrichtentextbuchstaben zu erhalten.

### 5.2.3 Brechen des Systems



Natürlich liefert die Mathematik ein Verfahren zum Brechen des Vigenere-Systems: Angenommen die Schlüsselwortlänge beträgt 3. Dann wird der 1., 4., 7., 10., ... Buchstabe des Nachrichtentextes stets mit dem-

selben Schlüsselwortbuchstaben verschlüsselt, so dass eine monoalphabetische Verschlüsselung vorliegt. Entsprechendes gilt für den 2., 5., 8., ... Buchstaben und für den 3., 6., 9., ... Buchstaben. Man erhält die Schlüssellänge als größten gemeinsamen Teiler der Abstände gleicher Buchstabenblöcke im Geheimtext. Es kommt häufiger vor, dass gleiche Nachrichtensequenzen mit dem gleichen Schlüssel verschlüsselt werden, so dass identische Buchstabenblöcke im Nachrichtentext entstehen, deren Abstand ein Vielfaches der Schlüssellänge ist. Im Geheimtext muss also nach gleichen Buchstabenblöcken gesucht und deren Abstand bestimmt werden. Das Programm ermittelt dann jeweils den ggT zweier Abstände und gibt diese aus. Dann gibt man die

vermutliche Schlüssellänge ein, das Programm schlägt ein Schlüsselwort vor, mit dem der Text entschlüsselt wird.

### 5.3 Das Knapsack-System

Das Knapsack-System ist ein asymmetrisches Verfahren, das heißt, dass Sender und Empfänger verschiedene Schlüssel zum ver- und entschlüsseln benutzen. Diese Schlüssel müssen natürlich mathematisch zusammen passen, sonst ist eine Entschlüsselung unmöglich. Der Schlüssel zum Verschlüsseln kann zudem von jedem in einer Art Telefonbuch nachgeschlagen werden, ist also nicht geheim. Der Schlüssel zum Entschlüsseln muss dagegen geheim gehalten werden. Also muss man dafür sorgen, dass man aus diesem öffentlichen Schlüssel nicht den geheimen Schlüssel ermitteln kann.

Umgekehrt muss es aber einfach sein, von dem geheimen Schlüssel auf den öffentlichen Schlüssel zu schließen, denn die beiden Schlüssel müssen ja zusammen passen. In die eine Richtung zu gehen muss also schwer sein, in die andere leicht. Dies ist prinzipiell beim Multiplizieren der Fall: Zwei große Zahlen zu multiplizieren geht sehr schnell, aber aus einer großen Zahl die Faktoren zu ermitteln dauert sehr lange. Mit einer großen Zahl sind hier etwa 500-stellige Zahlen gemeint.

Das Knapsack-System beruht darauf, einen Rucksack mit vorgegebenem Fassungsvermögen mit Packstücken mit vorgegebenem Volumen zu packen. Anders ausgedrückt: Gegeben sei das Rucksackvolumen 64 und die Packstücke 34, 31, 28, 22, 13, 8, 6, 2. Welche Packstücke muss man verwenden? Dies ist nicht leicht zu beantworten, vor allem, wenn das Rucksackvolumen in der Größenordnung von mehreren Billionen liegt und man ca. eine Millionen Packstücke zu testen hat. Haben die Packstücke dagegen eine besondere Eigenschaft, so ist es ganz einfach: Gegeben sei das Rucksackvolumen 64 und die Packstücke 56, 28, 14, 8, 3, 2. Warum muss wohl die 56 auf jeden Fall dabei sein (Tipp: Berechne die Summe der restlichen Zahlen!)?

### 5.3.1 Produkt



Das Programm berechnet das Produkt beliebig großer Zahlen. Dazu werden die Ziffern einer Zahl in Arrays gespeichert und miteinander schriftlich multipliziert.

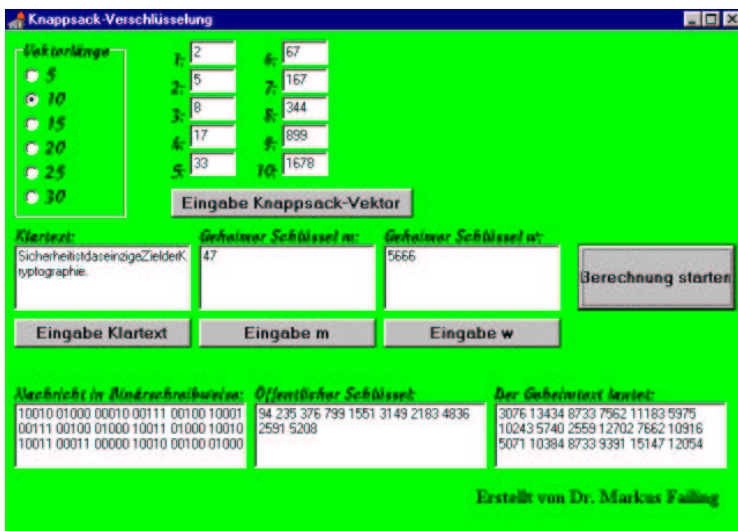
### 5.3.2 Faktorisierung

Die Faktorisierung einer Zahl dauert sehr lange. Man muss prinzipiell alle Teiler ermitteln, also die Zahl durch 1, 2, 3, 4, ... teilen und jeweils ermitteln, ob die Division ganzzahlig ist. Mathematiker haben herausgefunden, dass es reicht, durch alle Primzahlen bis zu einer



Grenze zu teilen, die etwa bei der Wurzel der zu faktorisierenden Zahl liegt. Die vereinfacht die Berechnung bereits erheblich, die Zeit, in der eine 500-stellige Zahl mit einem handelsüblichen 1,3 GHz-Rechner faktorisiert werden kann, beträgt mehrere Milliarden Jahre

### 5.3.3 Verschlüsselung



Zu Beginn des Programms gibt man die Anzahl der Packstücke an (oben wurden zehn Packstücke verwendet). Anschließend wird

der Klartext und zwei geheime Schlüssel eingegeben. Den Rest erledigt das Programm. An dieser Stelle kann der vollständige Algorithmus nicht erläutert werden. Für Nachfragen steht der Autor gerne zur Verfügung.

Ein Programm zur Entschlüsselung und zur Kryptoanalyse steht momentan nur im Pascal-Code zur Verfügung, muss also noch in den Delphi-Code übertragen werden.