MATHEMATIK IN DER KRYPTOGRAPHIE

VON
HERMANN KAUTSCHITSCH
UNIVERSITÄT KLAGENFURT

Dieser Beitrag kann für den Mathematikunterricht in verschiedenster Weise verwendet werden:

1. Die Kryptographie liefert zahlreiche Beispiele für eine anwendungsorientierte Mathematik, wobei die Anwendung nicht wirklichkeitsfremd oder gekünstelt wirkt, vor allem ist sie altersgemäß.
2. An Hand der Kryptographie kann der Schüler in die Prinzipien des Mathematisierens eingeführt werden.
3. Der Beitrag liefert eine Diskussionsgrundlage zum Thema: Reine Mathematik versus Angewandte Mathematik. Er zeigt, daß manche Ergebnisse der "reinen" Mathematik (hier vor allem der Zahlentheorie), noch nach Jahrhunderten "lebenswichtige" Anwendungen finden. So erweist sich die Mathematik des 20. Jahrhunderts (dem Schüler!) nicht als tote Wissenschaft, die nur aus Axiomatik und Verwaltung der alten Sätze besteht.
4. Die Beispiele erfordern teilweise einen sinnvollen Einsatz des Taschenrechners, eines Mikrocomputers und der Gruppenarbeit.
5. Die Beispiele liefern eher unübliche, dafür aber vielleicht desto wirksamere Motivationen für Begriffsbildungen aus der reinen Mathematik, die sonst im traditionellen Mathematikunterricht eher stiefmütterlich behandelt werden.
   Die folgende Tabelle gibt einen Überblick:

Mathematikscher Inhalt	Chiffrier- und Dechiffriermethoden
Funktionen, Kompositionen von FKT., Inverse Funktion Fixpunkte	Chiffrieren, dechiffrieren RSA-Chiffrierprinzip
Permutationen Rechnen mit Permutationen	Transpositionsmethode
Mehrdeutige Zuordnung	Polyalphabetische Verschlüsselung
Statistische Methoden Häufigkeit	Buchstaben-Frequenz-Sequenz-Analyse
Rechnen mit Wahrscheinlichkeiten	Friedmann-Kappa-Test Kerckhoffs-Überlagerungen
Irrationalzahl Rechnen mit Irrationalzahlen Numerik	Vernam-Methode "Zahlenwurm"-Methode
Kongruenz Rechnen mit Kongruenzen	Vernam-Methode RSA-Prinzip Pseudozufallszahlen
Primzahl, Vielfache, große Primzahlen, Primzahltests	RSA Faktorenanalyse von Karsiski
Fundamentalsatz der Zahlentheorie Satz vom g.g.T.	RSA-Prinzip

Fundamentalsatz
Euklidischer Algorithmus
Lineare Diophantische Gleichungen

Kleiner Fermatscher Satz
"Gruppentheorie"

RSA-Prinzip

Schema für den Prozeß des Mathematisierens (nach H.G. STEINER):

(i) Vertrautmachen mit der Situation
(ii) Entwurf eines pragmatischen Ansatzes, mit dem das Problem ohne allgemeine Theorie behandelt werden kann. Durch wiederholte Rückkoppelung an die gegebene Situation und eventuelle Kritik wird der Ansatz ständig verbessert.
(iii) Formulierung des mathematischen Problems
(iv) Lösung des mathematischen Problems
(v) Interpretation der Lösung
(vi) Vergleich mit der Wirklichkeit, eventuelle Verfeinerung der mathematischen Instrumente
(vii) Einbau der mathematischen Methoden in größere mathematische Zusammenhänge und allgemeine Theorien
(viii) Anwendung der entwickelten mathematischen Instrumente auf weitere Probleme innerhalb und außerhalb der Mathematik

An Hand der Kryptographie wollen wir dieses Schema realisieren:

(i) Zur Situationsbeschreibung:
Beispiele zur Bedeutung der Chiffrierung und der Dechiffrierung

1) Französische Kryptoanalytiker führten entscheidende Wende im 1. Weltkrieg herbei

2) Eintritt der USA in 1. Weltkrieg hervorgerufen durch Entschlüsselung ("Zimmermann-Depesche")

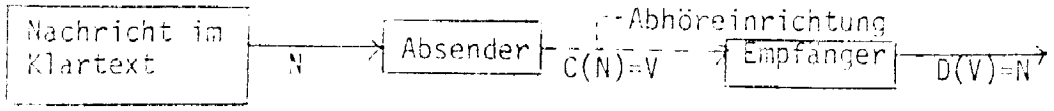
3) 2. Weltkrieg hätte ohne die bei den Alliierten so erfolgreiche Funkaufklärung 1-2 Jahre länger gedauert (? Atombombe über Deutschland)

4) Auch heute spielen geheime Nachrichten eine große Rolle - Spionage (Ausweisung russische Diplomaten aus Frankreich hervorgerufen durch Knacken eines elektrischen Codes)

5) Computerkriminalität:
1/2 Million Dollar durch Einstreichen der Nachkommastellen
50.000 DM Kindergeld für nichtexistierende Kinder
Diebstahl von Kundenlisten, Plänen
Französischer Zoll besorgte sich Kontonummern französischer Staatsbürger von Konten in Basel

6) Datenschutz sensibler Daten
Computer trägt zur Verwirklichung demokratischer Ideale bei, zur Sicherung der Privatsphäre, zur Befreiung von Überwachung und Kontrolle des einzelnen. Andererseits würde ein perfekter Datenschutz eine internationale Kontrolle überhaupt erst ermöglichen (Atomsperrvertrag! Rüstungskontrolle!)

(ii) Entwurf eines pragmatischen Ansatzes:



Mathematische Modellierung

Nachricht ..... Endliche Folge N von Buchstaben
Verschlüsselung ..... Chiffrierfkt. C
verschlüsselte Nachricht ..... C(N)=V: Ziffernfolge, oder Buchstabenfolge
Entschlüsselung ..... Dechiffrierfkt. $D=C^{-1}$
Dechiffrierte Nachricht ..... D(V)=(DoC)(N)=N

Außermathematische Motivation der Begriffe Funktion, Umkehrfunktion, Zusammensetzung von Funktionen

Man unterscheidet zwei Hauptverfahren:

TRANSPOSITIONSVERFAHREN:
Buchstaben in der ursprünglichen Form übernommen
Geändert wird die Reihenfolge
Angegeben durch einen Vertauschungszyklus

Motivation für "PERMUTATION" und "RECHNEN mit PERMUTATIONEN"

$C: (43251) \triangleq \begin{pmatrix} 12345 \\ 43251 \end{pmatrix}$

Klartext in 5-Gruppen anschreiben

Klartext: Ankunft von Peter abwarten

TRANSKRIPTION:

ANKUN		NKNAU
FTVON		NVTFO
PETER	C	RTEPE
ABWAR	$\longrightarrow$	RWBAA
TEN		NET

Kryptogramm: NKNAU NVTFO RTEPE RWBAA NET

$D=C^{-1}: \begin{pmatrix} 12345 \\ 43251 \end{pmatrix}^{-1} = \begin{pmatrix} 43251 \\ 12345 \end{pmatrix} = \begin{pmatrix} 12345 \\ 53214 \end{pmatrix}$

D:(53214)

NKNAU		ANKUN
NVTFO		FTVON
RTEPE	D	PETER
RWBAA	$\longrightarrow$	ABWAR
NET		TEN

Die drei überzähligen Buchstaben kommen auf die Stellen
1 $\longrightarrow$ 4
2 $\longrightarrow$ 3
3 $\longrightarrow$ 2 also NET auf 234
1...5 bleibt leer.

SUBSTITUTIONSVERFAHREN

Jeder Buchstabe wird duch ein Geheimzeichen ersetzt, die Reihenfolge bleibt gleich.

Cäsar-Alphabet: Alphabete gegeneinander verschoben

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

Motivation für "BIJEKTIVE FUNKTION"

Monoalphabetische Methode

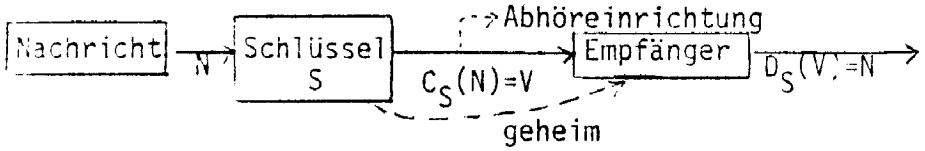
Klartext: Die chemische Formel
Kryptogramm: mrnlqnvrblqnoxavnu

1. Kritik:
a) Die gesamte Chiffrierfunktion muß geheimgehalten werden
b) "Leichte" Entzifferung - das Schlüsselalphabet hat eine zu große Ordnung
   Jede Sprache hat charakteristische Prozentsätze, in denen die einzelnen Buchstaben auftreten
   Sprachstatistik - EDV-Einsatz
   Deutsch: e
   Romanisch: a
   Russisch: o
Es gibt Tabellen für Zweiergruppen, Dreiergruppen,...., Doppelbuchstaben
"STATISTISCHE METHODEN"
"HÄUFIGKEITEN"
"STATISTISCHES GRFÜHL"

Ergebnisse der Sprachstatstik gelten zunächst nur für Klartext. In verdeckter Form tauchen sie im Kryptogramm auf. Bei Transpositionen unverändert - bei Cäsaralphabeten verschoben. STATISTIK ermöglicht Unterscheidung zwischen Transpositions- und Substitutionsverfahren.
Bei willkürlichen, jedoch monoalphabetischen Methoden findet man dieselbe Verteilung.

2. Verbesserung:
Einsatz eines "Schlüssels"= Folge von Ziffern oder Buchstaben
Zur Chiffrierung bzw. Dechiffrierung benötigt man auch den Schlüssel, zur Erzielung größerer Verwirrung wird er oft gewechselt. Dient auch als Gedächtnishilfe, um sich nicht das ganze Schlüsselalphabet zu merken:

SCHEMA



Nachricht ..... Endliche Folge von Buchstaben: N
Schlüssel ..... Endliche Folge von Zahlen, Buchstaben
Verschlüsselung ..... Chiffrierfunktion C_S
Kryptogramm ..... Endliche Folge $C_S(N)=V$
Entschlüsselung ..... Dechiffrierfunktion $D_S=C_S^{-1}$
Entschlüsselte N..... $N=D_S(V)=D_S(C_S(N))=(D_S \circ C_S)(N)=Id(N)=N$

Beispiele:

a) Transpositionsverfahren: Schlüsselwörter für komplizierte Umstellungen; diese merkt man sich (keine Notiz!)

K A T Z E N A U G E
6 1 8 10 3 7 2 9 5 4

b) Substitutionsmethode: Den ersten Buchstaben des Klartextalphabets werden der Reihe nach die Buchstaben des Schlüsselworts eingesetzt (z.B. KATZE)

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

Um die charakteristischen Buchstabenhäufungen zu vermeiden, verwendet man "polyalphabetische Verschlüsselungen": Einem Buchstaben des Klartextalphabets wird nicht ein einziger Buchstabe zugeordnet, sondern mittels eines Schlüsselwortes mehrere.

Motivation für "MEHRDEUTIGE ZUORDNUNG"

Beispiel: 4-deutige Zuordnung
Klartext: Zwölf Stunden Sendepause

Klartextalphabet	Schlüsselwort			
	F	E	L	D
A	20	46	65	97
B	21	47	66	98
C	22	48	67	99
D	23	49	68	75
E	24	25	69	76
F	00	26	70	77
G	01	27	71	78
I	02	28	72	79
J	03	29	73	80
K	04	30	74	81
L	05	31	50	82
M	06	32	51	83
N	07	33	52	84
O	08	34	53	85
P	09	35	54	86
Q	10	36	55	87
R	11	37	56	88
S	12	38	57	89
T	13	39	58	90
U	14	40	59	91
V	15	41	60	92
W	16	42	61	93
X	17	43	62	94
Y	18	44	63	95
Z	19	45	64	96

Verschlüsselte Alphabete

Verschlüsselter Text: 64168 52405 77125 89133 75240 71225 33682 40997 14382 4

Der erste Buchstabe F des Schlüsselwortes gibt an, daß 00 F zugeordnet wird, 25 dem Buchstaben E in der zweiten Spalte usw. Um mit zweistelligen Zahlen auszukommen, wurde ein Alphabet mit 25 Buchstaben zugrunde gelegt (I=J). Um die typischen Buchstabenfrequenzen zu vermeiden, wählt man die Zuordnung zu den 4 Spalten vollkommen willkürlich.

Bei der polyalphabetischen Verschlüsselung verwendet man also mehrere Alphabete. Man benützt dabei eine Tabelle aus 26 untereinander stehender Alphabete, von denen das zweite mit einem b, das dritte mit einem c usw. anfängt.

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
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 a
.
.
.

Den ersten im Klartext auftretenden Buchstaben sucht man in der ersten Zeile auf und verschlüsselt ihn durch den darunterstehenden Buchstaben, den zweiten Buchstaben verschlüsselt man durch die 3. Zeile usw. Insgesamt hat man eine 25-wertige Zuordnung. Dieses Prinzip des sukzessiven Wechsels von Buchstabe zu Buchstabe verwendet man auch bei den modernen elektronischen Schlüsselmaschinen.

Im Sinne der ersten Kritik verwendet man auch Schlüssel: Um die Reihenfolge der eingesetzten Schlüsselalphabete zu kennzeichnen, verwendet man auch Schlüsselwörter. Siehe dazu das weiter unten stehende Beispiel mit dem Schlüsselwort NATUR.

FAKTORENANALYSE von KASISKI:
Entschlüsselung eines Polyalphabetischen Systems mit periodischem Schlüsselwort.

Mathematische Mittel: PRIMZAHLENDARSTELLUNG; VIELFACHE

Bei monoalphabetischen Systemen werden gleiche Buchstabenpaare stets durch gleiche Buchstabenpaare ersetzt.
Bei polyalphabetischen Systemen ist das i.a. nicht mehr der Fall, es sei denn: Die betreffende Buchstabengruppe liegt zufällig auch an derselben Stelle einer Periode (z.B. 5 bei NATUR). Die Zahl der Entsprechungen sinkt dann auf ein Fünftel. Dann weiß man, daß es sich um ein Schlüsselwort aus 5 Buchstaben gehandelt hat.

Beispiel aus dem Buch: Die geheime Nachricht(S. 70)

g e b r a u c h s a n w e i s u n g f u e r n e u e s i n f o r
N A T U R N A T U R N A T U R N A T U R N A T U R N A T U R N A
S D H W I G B N X I Z V K N A G M M K C Q Q T J C Q R O S N A Q

m a t i o n s s y s t e m n i c h t e i n g e t r o f f e n t e
S F B U N T X A K R Z J U Z H I M B Q H T L M F Q U K N Q M Z J

r m i n f u e r g e p l a n t e a k t i o n m u s s u m m i n d
Z Y H T K C Q Q M J X X Z T Y M M J Z N W Z L A X A G L S N V P

e s t e n s z w e i w o c h e n v e r s c h o b e n w e r d e n
D Y Y M A R F B M U V U H P Q M B J Z E B N T J Q M C J Z P D T

Als Ergebnis erhalten wir:

s d h w i g b n x i z v k n a g m m k c q q t j c
q r o s n a q s i b u n t x a k r z j u z h i m b
q h t i m f q u k n q m z j z y h t k c q q m j x
x z t y m m j z n w z l a x a g l s n v p d y y m
a r f b m u v u h p j m b u z e b n t j q m c j z
p d t

Als nächstes nimmt man üblicherweise die Bigramme auf:

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

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

Worauf es ankommt, sind die Abstände, die doppelt oder mehrfach auftretende Bigramme im verschlüsselten Text haben. Das Ergebnis der Auszählung ist:

Abstände Bigramme											
N A	16	Z J	20	Q M	49	C Q	45	J Z	60
X A	50	M J	7	Q M	10	C Q	40	J Z	32
F B	69	M M	64	Y M	20	Q Q	45	J Z	42
K C	50	Q M	11	B N	110	N T	81	J Z	10
P D	30	Q M	50	K N	46	H T	20		
A G	75	Q M	60	S N	4	J Z	18		
T J	96	Q M	39	C Q	5	J Z	50		

Und nun erfolgt die Zerlegung in Faktoren – von der Schule her als »Primzahlzerlegung« bekannt:

Faktorenzerlegung

16 = 2.2.2	7 = 7	20 = 2.2.5	81 = 3.3.3.3
50 = 2.5.5	64 = 2.2.2.2.2.2	110 = 2.5.11	20 = 2.2.5
69 = 3.23	11 = 11	46 = 2.23	18 = 2.3.3
50 = 2.5.5	50 = 2.5.5	4 = 2.2	50 = 2.5.5
30 = 2.3.5	60 = 2.2.3.5	5 = 5	60 = 2.2.3.5
75 = 3.5.5	39 = 3.13	45 = 3.3.5	32 = 2.2.2.2.2
96 = 2.2.2.2.2.3	49 = 7.7	40 = 2.2.2.5	42 = 2.3.7
20 = 2.2.5	10 = 2.5	45 = 3.3.5	10 = 2.5

Aufgrund dieser Tabelle ist die Auswertung leicht gemacht:

Vielfache von 2 kommen 22x vor
Vielfache von 3 kommen 12x vor
Vielfache von 4 kommen 11x vor
Vielfache von 5 kommen 18x vor
Vielfache von 6 kommen 6x vor
Vielfache von 7 kommen 3x vor
Vielfache von 8 kommen 5x vor
Vielfache von 9 kommen 4x vor
Vielfache von 10 kommen 13x vor
Vielfache von 11 kommen 2x vor
Vielfache von 12 kommen 3x vor
Vielfache von 13 kommen 1x vor
Vielfache von 14 kommen 1x vor
Vielfache von 15 kommen 6x vor

Daß Vielfache von 2 am häufigsten vorkommen, liegt daran, daß alle großen Zahlen Vielfache von 2 sind. Die Bestandsaufnahme weist deutlich auf eine Periodität von 5, der Anzahl der Buchstaben des Wortes NATUR, hin.

In der Praxis sind die Rechnungen noch viel langwieriger, daher Einsatz von Mikrocomputern.

2. Verbesserung:
Nicht periodisch eingesetzte Schlüsselwörter

Jede neue Nachricht beginnt man an einer anderen Stelle des Schlüsselwortes.

Zur Entschlüsselung: Überlagerungsmethode
Man legt mehrere Kryptogramme untereinander
periodisch: Alle in einer Kolonne stehenden Zeichen gehören demselben Schlüsselalphabet an ⟶ STATITISTISCHE METHODEN
nicht periodisch: Kolonnen verschieben, bis sie ein und demselben Buchstaben des Schlüsselwortes entsprechen
Wie?
FRIEDMANN'sche KAPPA-Test

Motivation für: WAHRSCHEINLICHKEITSTHEORIE
RECHNEN mit WAHRSCHEINLICHKEITEN

$$P\text{ (gleichzeitiges Auftreten von 2 zufälligen Buchstaben)} = \frac{1}{26.26} = \frac{1}{736}$$

$$P\text{ (beliebiges Buchstabenpaar)} = \frac{1}{26} = 0{,}0385 =: \varkappa_R$$

In der menschlichen Sprache treten Buchstaben nicht nach einer Zufallsverteilung auf, sondern haben charakteristische Häufigkeiten.

P(aa)=0,0781.0,0781 = 0,0061
P(bb)=0,0128.0,0128 = 0,0002
.
.
.
P(zz)= = ...

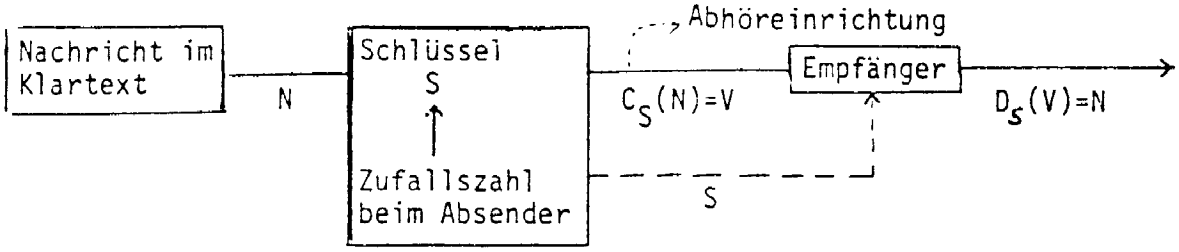
P(beliebiges Buchstabenpaar)=0,0738=: $\varkappa_p$

Unterscheidungsmöglichkeit zwischen sinnlosem Text und sinnvollem Text durch höheren Kappawert

4. Verbesserung:
keine Schlüsselwörter, sondern Zufallsfolgen

Zur Erhöhung der Sicherheit wird der Schlüssel (=Ziffernfolge) von Fall zu Fall verändert (Zufallszahlengenerator)

Schema:



Mathematische Modellierung

Nachricht ..... Endliche Folge von Buchstaben: N
Schlüssel ..... Endliche Zufallsfolge S
Verschlüsselung ..... Chiffrierfunktion C_S
verschlüsselte Nachricht ..... Zifferfolge (Zufallsfolge): $C_S(N)=V$
Entschlüsselung ..... Dechiffrierfunktion D_S
Entschlüsselte Nachricht ..... $N=D_S(V)=(D_S \circ C_S)(N)=N$

Der Schlüssel verwandelt die chiffrierte Nachricht in eine Folge von Zufallszahlen um

Beispiel:
Ein-Weg-Schablone mit Zufallsziffern (VERNAM-Methode)

Man kann nachweislich nicht aus der Kenntnis von N und $C_{S(N)}=V$ die Chiffrierfunktion C_S berechnen.

Absender A erzeugt durch Münzenwurf eine binäre Folge S=00100110...
C: Jeder Buchstabe durch seine Nummer im Alphabet ersetzt, als binärer 5-Block geschrieben
N=NEIN≙14050914≙ $\underbrace{11100010101001011 10}_{C(N)}$

Für S wählt man die ersten 20 Ziffern der Zufallsfolge und addiert sie zu C(N) mit 1+1=0 (Restklassenaddition $\oplus_2$).
Es ist $S \oplus_2 S=00....0$

$V=C_S(N)=C(N) \oplus_2 S=01010100110101111101$

Der Empfänger bildet:
$D_S(V)=V \oplus_2 S=C(N) \oplus_2 S \oplus_2 S=C(N) \oplus_2 \overline{0}=C(N)$
anschließend $D\left[C(N)\right]=N$

Außermathematische Anwendung von: Zufallszahlen, Kongruenzrechnung, Zusammensetzung von Funktionen

Kritik:
1) Sicherheit hängt von der Geheimhaltung des Schlüssels ab (langsam und teuer)
2) Da Empfänger und Absender denselben Schlüssel benützen, kann sich der Empfänger selbst Nachrichten zusenden und behaupten, sie kämen vom Absender: Die Authen ität einer Nachricht ist nicht gewährleistet.
3) Langer Schlüssel: umständlich

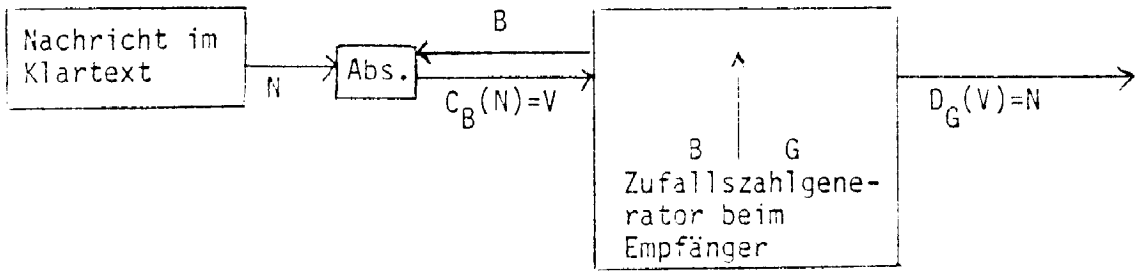
Gesucht: Methode zur Erzeugung langer, ungeordnet scheinender Ziffernfolgen. Dazu eignen sich Rechenoperationen, mit denen man relativ einfache Zahlen in höchst komplizierte Ausdrücke umformen kann.

Motivation für: IRRATIONALZAHL, RECHNEN mit IRRATIONALZAHLEN
NUMERISCHE METHODEN

$\sqrt{p}$, $\sqrt[m]{N} \in Q \Rightarrow N=a^m$, $a \in Z$
log 2 $\notin Q$, e^x *irrational für* $x \in Q$
$\pi^2 \notin Q$, $\tan \frac{m}{n} \notin Q \Rightarrow \pi \notin Q$
PSEUDOZUFALLSZAHLEN; KONGRUENZMETHODEN

Vierte Verbesserung des Modells

Zufallszahlengenerator beim Empfänger
2 Schlüssel: (B) öffentlich bekannter Schlüssel
(G) geheimer Schlüssel, den nur der Empfänger (bzw. sein Computer) kennt.



$C_B(N)=B\left[C(N)\right]=(BoC)(N)=V$

$D_G(V)=D\left[G(V)\right]=(DoG)(V)=N$

Es muß gelten:
GoB=I, I identisch Funktion

Insgesamt

$$N \xrightarrow{C} C(N) \xrightarrow{B} (BoC)(N)=V \xrightarrow{G} (GoB)\left[C(N)\right]=C(N) \xrightarrow{D} N$$

Buchstabenfolge — Zahlenfolge — Zufallszahlenfolge

Motivation für "ZUSAMMENSETZEN von FUNKTIONEN"

Einwand: Wenn BoG=I sein soll, dann kann man prinzipiell aus B die dazu inverse Funktion G berechnen!

TRICK: Die Funktion B ist so beschaffen, daß man ihre Funktionswerte schnell berechnen kann, es ist aber "hoffnungslos" schwer, ihre Umkehrung zu berechnen (auch mit den derzeitigen Computern)

Das System ist nicht mathematisch sicher, sondern "nur" rechnerisch sicher.

Auch wenn der Absender den Empfänger nicht kennt, kann er ihm eine vertrauliche Nachricht zusenden: Er besorgt sich aus dem öffentlich zugänglichen "Buch" den öffentlichen Schlüssel B_E des Empfängers, tippt am Terminal die Nachricht N. Der Computer verschlüsselt sie automatisch und sendet an E die Nachricht $V=C_{B_E}(N)=(B_E o C)(N)$.

Nur der Computer von E besitzt den Schlüssel G_E. Er bildet:

$$D_{G_E}(V)=\left[Do(G_E o B_E)oC\right](N)=(DoC)(N)=N$$

Die Authenzität der Nachricht kann gesichert werden. Für die inverse Funktion gilt auch BoG=I.

Der Absender A signiert seinen Auftrag:
Er wendet auf N zuerst seinen nur ihm bekannten Schlüssel G_A an und dann B_E.
Es ist also

$$V=\left[B_E o G_A oC\right](N).$$

Der Empfänger E wendet zuerst den nur ihm bekannten Schlüssel G_E, und dann den öffentlichen Schlüssel B_A, anschließend die inverse Chiffrierfunktion D:

$$\left[DoB_A oG_E\right](V)=\left[DoB_A oG_E oB_E oG_A oC\right](N)=(N)$$

E weiß, daß nur von A die Nachricht gekommen ist, denn nur A kennt G_A. Nur E kann die Nachricht lesen, denn nur E kennt G_E. (Zumindest in einer vernünftigen Zeit).

Damit scheint der pragmatische Ansatz nicht mehr verbesserungsfähig zu sein. Wir haben demonstriert, wie man durch wiederholte Rückkoppelung an die gegebene Situation den Ansatz ständig verbessern kann.

(iii) Formulierung des mathematischen Problems:

Wir suchen Funktionen, deren Funktionswerte relativ schnell berechenbar sind, die eine gegebene Nachricht N möglichst stark verändern und die umkehrbar sind. Die Umkehrfunktion soll aber nur mit einem hohen Aufwand an Rechenzeit gefunden werden können. Das Anwenden der Umkehrfunktion für den rechtmäßigen Empfänger soll dagegen wieder schnell möglich sein.

(iv), (v) Lösung des mathematischen Problems und Interpretation:

RIVEST, SHAMIR, ADLEMANN: RSA-System

Aufgabe: Große Zahl n faktorisieren
Zur Lösung benötigt man eine mit der Stellenanzahl exponentiell anwachsende Rechenzeit, Probe schnell durchführbar.

Beispiel: n = 29083
n = 127.229
Die Lösung beruht im Prinzip auf dieser Primzahlzerlegung.

Chiffriervorgang:

1. Nachricht N als natürliche Zahl n dargestellt. Digitales Alphabet: Jedem Symbol 2 Ziffern zugeordnet: C(N)=n

a=00	b=01	c=02	.....	z=25
A=26	B=27	C=28	.....	Z=51
0=52	1=53	2=54	.....	9=61
=62	.=63	,=64	;=65	?=66,...

Nur n zu übermitteln wäre sinnlos, als Chiffrierfunktion wählen wir die Potenzfunktion n^i, wobei so wie früher, i eine Zufallszahl sein soll. Da die Funktion monoton wachsend ist, könnte man die Funktion leicht invertieren. Durch Einführung der Kongruenzrechnung mod m erreicht man größere Verwirrung, man wandelt die monoton wachsende Zahlenfolge in eine scheinbar ungeordnete Folge um.

Außermathematische Motivierung der Kongruenzrechnung an einem echten Problem.

Beispiel: m=11, i=3

n	0	1	2	3	4	5	6	7	8	9	10
$v'=n^3$	0	1	8	27	64	127	216	343	512	729	1000
$v\equiv n^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

Modulfunktionen sind ein Instrument der Verwirrung.

Es gibt gute Algorithmen für schnelles Potenzieren:
Fortgesetztes Quadrieren und gelegentliches Multiplizieren mit a.

$$8^{27}=8^1.8^2.8^8.8^{16}$$

Modulmultiplikationen verhindern das Auftreten großer Zahlen, um 8^{27} zu berechnen, benötigt man nur 7 Modulmultiplikationen. Ein schlechter Algorithmus wäre fortgesetztes Multiplizieren.

Natürlicher Einstieg zum Problemkreis "Algorithmen". Sinnvolle Verwendung von Taschenrechnern und Mikrocomputern.

Hauptproblem: Wie findet man die Umkehrfunktion von $n \to n^i \equiv v \pmod m$?
Sie muß injektiv sein, aus $n_1 \not\equiv n_2 \pmod m$ muß also $n_1^i \not\equiv n_2^i \pmod m$ folgen.

Motivation für INJEKTIVITÄT

Nach NÖBAUER:
Ein Polynom bewirkt genau dann eine Permutation des Restklassenringes mod $m=p_1.p_2. \ldots p_r$, wenn dies auch mod $p_1,\ldots$ mod p_r geschieht. Mod p, p prim, hat nun $x^i \equiv u(p)$ genau dann eine Lösung, wenn $d=ggT(i,p-1)$ ein Teiler vom Index von u ist. Da dies für alle u gelten muß, ist d=1. n^i bewirkt also genau dann eine Permutation vom Restklassenring mod p, wenn ggT(i,p-1)=1 ist.

"Alte" Resultate aus der reinen Mathematik finden Anwendungen.

Da man für die Berechnung von Potenzen einen schnellen Algorithmus kennt, versuchen wir, für die Umkehrfunktion eine Potenzfunktion zu nehmen (nur 1 chip notwendig). Dann müßte es eine Zahl j geben, mit

$$(*) \qquad v^j=n^{ij} \equiv n \pmod m.$$

Assoziation mit dem KLEINEN FERMAT'SCHEN SATZ: $a^p \equiv a \pmod p$, p prim

Einfacher Induktionsbeweis:
Ist p prim, dann ist $\binom{p}{r} \equiv 0 \bmod p$, $0<r<p$, also ist $(a+b)^p \equiv a^p+b^p \bmod p$.
Nun ist $1^p \equiv 1 \bmod p$ und aus $a^p \equiv a \bmod p$ für alle a folgt

$(a-1)^p \equiv a^p+1^p \equiv a+1 \bmod p$.

Verwendet man diesen Satz in obiger Kongruenz (*), dann müßte m=p sein und i,j Potenzen von p, Umkehrfunktion wäre leicht zu berechnen.

Wir setzen m nicht als prim voraus.
Sei m=p.q, p,q prim.
Wir wollen den Fermat auf diesen Fall verallgemeinern:

$a^p \equiv a \bmod p \Leftrightarrow p/a.(a^{p-1}-1)$

Fundamentallemma der Zahlentheorie:

$$\boxed{p/Z_1.Z_2,\ p\not/Z_1 \Rightarrow p/Z_2}$$

Ist also a nicht durch p,p teilbar, dann gilt

$$a^{p-1} \equiv 1 \bmod p$$
$$a^{q-1} \equiv 1 \bmod q$$
$$\Rightarrow a^{(p-1)(q-1)}=(a^{p-1})^{q-1} \equiv 1 \bmod p$$
$$a^{(q-1)(p-1)} \equiv 1 \bmod q$$

Da p,q prim, folgt daraus

$$\boxed{a^{(p-1)(q-1)} \equiv 1 \bmod (p.q)} \quad \text{oder}$$
$$a^{k(p-1)(q-1)} \equiv 1 \bmod (p.q)$$

1761 gelang es EULER, diesen Satz auf beliebige Modul zu verallgemeinern.
Anwendung:

$$\boxed{r \equiv s \bmod (p-1)(q-1) \Rightarrow a^r \equiv a^s \bmod p.q}$$

$r=s+k(p-1)(q-1) \Rightarrow a^r=a^{s+k(p-1)(q-1)} = a^s.a^{k(p-1)(q-1)} \equiv a^s \bmod p.q$

Verallgemeinerung: Kleiner Fermatischer Satz der Gruppentheorie (|G| ... Ordnung der Gruppe)

$$a^{|G|}=e$$

Damit kann jemand, der die zwei Primfaktoren p,q von m=p.q kennt, relativ schnell die Umkehrfunktion berechnen:

Man bestimmt eine Zahl j mit

$$i.j \equiv 1 \bmod (p-1)(q-1)$$

Dies ist eindeut möglich, wenn i zu (p-1)(q-1) teilerfremd ist. Dann ist auch n^i eine Permutation des Restklassenringes mod m=p.q, also existiert die Umkehrfunktion. Sie ist gegeben durch:

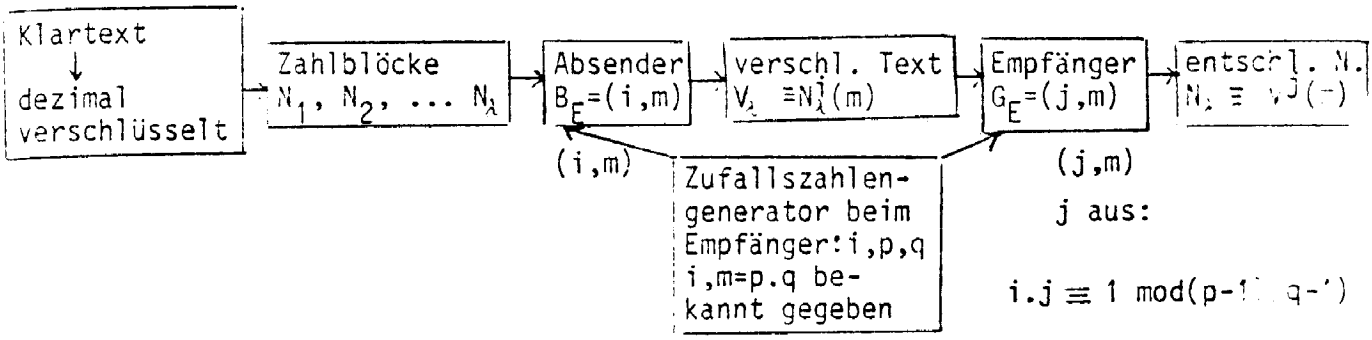
$$v^j=n^{i.j} \quad n^1 \bmod p.q.$$

Hier ergibt sich ein natürlicher Einstieg zur Lösung von linearen Kongruenzen $ax \equiv b \bmod m$, bzw. linearen diophantischen Gleichungen.

Insgesamt:
Wählt man für p und q zwei große Primzahlen, dann ist für jemandem, der die beiden Primfaktoren nicht kennt, nach bisherigen Erkenntnissen, es unmöglich, die Chiffrierfunktion in vernünftiger Zeit umzukehren. Das Chiffriersystem ist so sicher, wie die Faktorisierung.

(Wählt man z.B. für m eine 200 stellige Zahl, dann folgt aus den bisherigen Zerlegungsalgorithmen eine Zerlegungszeit von rund $3{,}3.10^8$ Jahren bei 10^6 Rechenschritten/sec.)

Schema:



Mathematische Modellierung (Interpretation der Lösung)

Nachricht ..... Endliche Folge von Restklassen mod m
öffentlicher Chiffrierschl. . Zahlenpaar (i,m), zufällig
Chiffrierfunktion ..... Modulfunktion $y=x^i \bmod m$
Dechiffrierfunktion ..... Modulfunktion $y=x^j \bmod m$
Dechiffrierschlüssel ..... Zahlenpaar (j,m)
Verschlüsselte Nachricht .... Zufallszahlenfolge

(vi) Verfeinerung der mathematischen Instrumente, Vergleich mit Wirklichkeit:

Durch unglückliche Wahl der Zahlen i,p,q kann es passieren, daß ein Zeichen des Klartextes auf sich selbst abgebildet wird (Fixpunkt), ja daß sogar ein Wort auf sich selbst abgebildet wird.

Motivation für FIXPUNKTFREIE ABBILDUNG

Aus Platzmangel kann auf die Beseitigung dieses Problems nicht eingegangen werden, man muß j doch j so bestimmen, daß

$$i.j \equiv 1 \bmod kgv[(p-1)(q-1)] \text{ ist.}$$

Eine zweite Gefahr besteht darin, daß bei unglücklicher Wahl von p,q jemand ohne die Kenntnisse von i auskommt.

(vii) Einbau der mathematischen Methoden in allgemeine Theorien:

Aus den bisherigen Überlegungen ist klar geworden, welche theoretischen Erkenntnisse und Rechenverfahren die Mathematik noch beisteuern muß:

1. Wir benötigen die Tatsache, daß jede natürliche Zahl sich eindeutig als Produkt von Primzahlen darstellen läßt (Fundamentalsatz der Zahlentheorie). Gäbe es nämlich für m=p.q noch eine zweite Primfaktorzerlegung (eventuell mit kleineren Primzahlen), dann wäre es möglich, daß man m doch in einer kurzen Rechenzeit faktorisieren könnte.

2) Wir haben entscheidend verwendet: Ist ein Produkt a.b durch eine Primzahl teilbar, dann ist es auch mindestens einer der Faktoren (Fundamenallemma).

3) Wir benötigen große Primzahlen. Primzahltests!

4) Wir benötigen das Rechnen mit Kongruenzen und das Lösungsverhalten von linearen Kongruenzen $ax \equiv b \pmod m$

5) Zufallszahlen, Algorithmen am Taschenrechner

Die meisten aufgezählten Probleme beschäftigen die Mathematiker schon seit der Antike, ohne daß irgendeine Anwendung (nicht einmal innerhalb der Mathematik) gesehen wurde. Die einzige Triebfeder der Forschung war die menschliche Neugier. Jetzt, praktisch nach Jahrtausenden, ergeben sich auch dafür echte Anwendungen.

(viii) Anwendung der mathematischen Instrumente auf weitere Probleme innerhalb und außerhalb der Mathematik

Fundamentalsatz: Bestimmen des g.g.T. und des k.g.V.
Teileranzahl
Mathematische "Zaubereien"
Perfekte Zahlen, Befreundete Zahlen

Kongruenzrechnung: Teilbarkeitsregeln, Mathematische "Zaubereien" (z.B. Geburtstag erraten), Rechenproben, Ewiger Kalender, Aufstellen von Turnierplänen, Periodische Dezimalzahlen (länge der Periode,.....) Erzeugung von Zufallszahlen

Lineare diophantische Gleichungen: Sachrechnen, Erweiterung auf pythagoräische Zahlentripel

Zufallszahlen: Wahrscheinlichkeitsrechnung, Monte-Carlo-Simulation

Beispiel zum RSA-Schema:

Klartext N: KOMME MORGEN
Dezimale Verschlüsselung C(N) nach Seite 12
C(N) = 364038383038404332303 9
p=19, q=29, m=551, i=17, (p-1)(q-1)=504
Öffentlicher Schlüssel (17, 551)
Wegen des Moduls m=551 zerlegen wir den Klartext in Dreierblöcke:

364 038 383 038 404 332 303 9

N_1

Verschlüsselte Nachricht: $N_1^{17} \bmod (551)$

$364^{17} \equiv 355 \pmod{551}$ usw.

V = 355 323 013 323 327 283 341 207

V_1 V_2

Bestimmen j aus $17.j \equiv 1 \bmod (504)$ oder $17.j-504.y=1$
Euklidscher Algorithmus liefert: $17.89-504.3=1$, also $j=89$
Geheimscher Schlüssel (89, 551)

$V_1^j = 355^{89} = 355^{64}.355^{25} \equiv 364 \bmod 551$

Analog: $V_2^j = 323^{89} \equiv 38 \bmod 551$

Mit dem SHARP PC-1211 rechnet man dies in wenigen Sekunden aus.

LITERATUR

ENGEL, A.: Datenschutz durch Chiffrieren: Mathematische und algorithmische Aspekte, MU, Jg. 25, Heft 6 (1979)

FRANKE, H.W.: Die geheime Nachricht, Umschau Verlag Frankfurt/Main (1982)

FISCHER, R.-MALLE, G.: Pädagogik für Lehrer an Höheren Schulen, Lehrbrief für das Fernstudium, Klagenfurt (1978)

HELLMANN, M.E.: Die Mathematik neuer Verschlüsselungssysteme, Spektrum der Wissenschaft (Oktober 1979)

NOBAUER, W.: Über eine Gruppe der Zahlentheorie, Monatshefts f. Math. 58 (1954), S 118

STEINER, H.G.: Zur Methodik des mathematisierenden Unterrichts, in Anwendungsorientierte Mathematik in der S II, Schriftenreihe Didaktik der Mathematik, Bd 1, UBW Klagenfurt (1976), Verlag J. Heyn, KLagenfurt

WEISS, J.: Zufallszahlen mit dem Taschenrechner MNU, Jg. 32, Heft 3 (1979)

WITTMANN, E.: Grundfragen des Mathematikunterrichts, 5. Auflage, Vieweg-Verlag Braunschweig (1978)