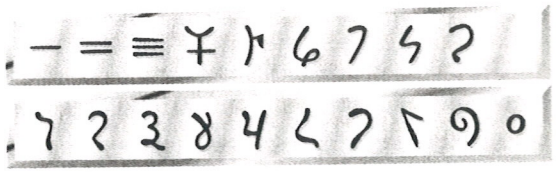
Technische Mathematik (Klagenfurt)
Faszination und Anwendung

Kryptographie - Wie schützt man elektronische Daten?

24. März 2009

Winfried B. Müller
Institut für Mathematik
Universität Klagenfurt



$x \longrightarrow f(x) \bmod 15$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x^3	0	1	8	12	4	5	6	13	2	9	10	11	3	7	14
$2x^3$	0	2	1	9	8	10	12	11	4	3	5	7	6	14	13
$g_3(-1,x)$	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
$g_{11}(-1,x)$	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1
f_5	0	4	8	12	1	5	9	3	2	6	10	14	3	7	11

Speicherung und Übertragung elektronischer Daten

- American Standard Code for Information Interchange (ASCII)
- Internationale Standard Buch Nummer (ISBN)
- Europäische Artikel Nummer (EAN)
- Identcode und Leitcodes der österreichischen Post
- Compact Disc und CD-ROM
- Elektronisches Grundbuch
- Elektronischer Zahlungsverkehr
  (Electronic Funds Transfer, Bankclearing, Electronic Commerce)
- Elektronische Geldbörse, Fahrscheine, Liftkarten, Mautkarten
  (Quick, KeyWatch, Kärnten Card)
- Elektronische Bankkarten, Ausweise, eCard,
  Telefonwertkarten, Studienbücher
- Elektronische Grenzkontrollen
  (US-Immigration, maschinenlesbarer Reisepaß)
- Fälschungssichere Theaterkarten, Lotterielose, Dokumente
- Satellitenkarten
- GPS-Anwendungen

1.3 Attacken, Sicherheitsdienste, Sicherheitsmechanismen

Threats – Attacken

- Identity Interception – illegales Beobachten der Identität eines Teilnehmers
- Masquerade – Vortäuschen einer falschen Identität
- Replay – Aufzeichnung und spätere Wiedergabe einer Nachricht
- Data Interception – illegales Mitlesen einer Nachricht
- Manipulation – Verändern einer Nachricht
- Repudiation – Verläugnen der Teilnahme an einer Kommunikation
- Denial of Service – Verhindern oder Unterbrechen einer Kommunikation
- Misrouting – Fehlleiten einer Nachricht
- Traffic Analysis – Beobachten der Kommunikation

Security Services – Sicherheitsdienste

- Access Control – Zutrittskontrolle
- Authentication/Authentification
- Data Confidentiality – Vertraulichkeit der Nachricht
- Data Integrity – Verhinderung der Verfälschung von Daten
- Notarization
- Non-repudiation – Empfangs- bzw. Absenderbestätigung
- Routing Control
- Timeliness

Security Mechanisms – Sicherheitsmechanismen

- Authentication Exchange – gegenseitige Identifikation
- Encipherment – Verschlüsselung
- Digital Signature – elektronische Unterschrift
- Timestamps – Zeitstempel

Modulare Arithmetik und Quellencodierung

Restklassenringe ganzer Zahlen

Beispiel: Uhrzahlen $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$+$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
...	...	...	...	...	...	...	...	...	...	...	...	...
11	11	0	1	2	3	4	5	6	7	8	9	10

Definition: Seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}^*$. Dann heißen die Zahlen a und b *kongruent bezüglich des Moduls* m, wenn $a-b$ durch m teilbar ist. Andernfalls heißen a und b zueinander *inkongruent* bezüglich m. Ist a kongruent zu b bezüglich m dann schreibt man

$$a \equiv b \bmod m.$$

Definition: Die Menge aller bezüglich eines festen Moduls m zueinander kongruenten Zahlen bildet eine sogenannte *Restklasse modulo* m.

Durch die folgenden Definitionen kann man auf einer Menge von Restklassen $\bmod m$ eine *Addition* und *Multiplikation* einführen:

$$\overline{a} \oplus_m \overline{b} := \overline{a + b}$$

$$\overline{a} \odot_m \overline{b} := \overline{a \cdot b}.$$

Restklassenring $< \mathbb{Z}_4; \oplus_4, \odot_4 >$

$\oplus_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\odot_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Körper $< \mathbb{Z}_2; \oplus_2, \odot_2 >=< GF(2); \oplus_2, \odot_2 >$

*	$\oplus_2$	$\overline{0}$	$\overline{1}$
	$\overline{0}$	$\overline{0}$	$\overline{1}$
	$\overline{1}$	$\overline{1}$	$\overline{0}$

$\odot_2$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Körper $< \mathbb{Z}_{11}; +, \cdot >=< GF(11); +, \cdot >$

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

$\cdot$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Schon im "sehr kleinen" Körper $< GF(11); +, \cdot >$ kann man demonstrieren, dass die Abbildung $x \rightarrow x^3$ eine Permutation induziert, welche die Elemente $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ "sehr gut verwirrt". Derartige Polynomfunktionen auf endlichen Körpern werden daher als Verschlüsselungsfunktionen auf der Menge der Elemente des Körpers eingesetzt.

x	0	1	2	3	4	5	6	7	8	9	10
$x^3 \bmod 11$	0	1	8	5	9	4	7	2	6	3	10

Ganz analog sieht man, dass die Inversenbildung $x \rightarrow x^{-1}$ eine Permutation auf der Menge der invertierbaren Elemente $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ von $GF(11)$ ist, welche die Elemente ebenfalls "sehr gut verwirrt".

x	1	2	3	4	5	6	7	8	9	10
$x^{-1} \bmod 11$	1	6	4	3	9	2	8	7	5	10

Keyboarding Errors

Fehlertyp	Symbol	Relative Häufigkeit in %
Einzel- oder Transskriptionsfehler	$a \rightarrow b$	79.1
Transpositonsfehler	$ab \rightarrow ba$	10.2
Übersprungener Vertauschungsfehler	$acb \rightarrow bca$	0.8
Zwillingsfehler	$aa \rightarrow bb$	0.5
Phonetische Fehler	$a0 \rightarrow 1a$ $(a = 2, \cdots, 9)$	0.5
Übersprungener Zwillingsfehler	$aca \rightarrow bcb$	0.3
Zufällige Fehler		8.6

Die Internationale Standard Buch Nummer (ISBN-Code)

Aufbau der ISB-Nummer:

a_1	$a_2a_3a_4$	$a_5a_6a_7a_8a_9$	a_{10}
Sprache	Verlag	Kennummer	Prüfziffer

Sind $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ die ersten neun Ziffern einer ISB-Nummer, dann wird die Prüfziffer a_{10} so berechnet, daß die "gewichtete" Summe

$$10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + 6 \cdot a_5 + 5 \cdot a_6 + 4 \cdot a_7 + 3 \cdot a_8 + 2 \cdot a_9 + 1 \cdot a_{10}$$

durch 11 teilbar ist.

BEISPIEL: Sind 3 528 28990 die ersten neun Stellen einer ISB-Nummer, dann muß die Prüfziffer $a_{10} = 2$ sein, da

$$10 \cdot 3 + 9 \cdot 5 + 8 \cdot 2 + 7 \cdot 8 + 6 \cdot 2 + 5 \cdot 8 + 4 \cdot 9 + 3 \cdot 9 + 2 \cdot 0 + 1 \cdot 2 = 264 = 11 \cdot 24$$

ENTDECKT: Einzelfehler

Transpositionsfehler

Übersprungene Vertauschungsfehler

Übersprungene Zwillingsfehler

Die Europäische Artikel Nummer (EA-Nummer)

Aufbau der EA-Nummer:

a_1a_2	$a_3a_4a_5a_6a_7$	$a_8a_9a_{10}a_{11}a_{12}$	a_{13}
Land	Hersteller	Kennummer	Prüfziffer

Die Prüfziffer a_{13} wird so berechnet, daß die "gewichtete Summe"

$$1 \cdot a_1 + 3 \cdot a_2 + 1 \cdot a_3 + 3 \cdot a_4 + \cdots + 1 \cdot a_{11} + 3 \cdot a_{12} + 1 \cdot a_{13}$$

durch 10 teilbar ist.

BEISPIEL: Sind 90 01375 00377 die ersten zwölf Stellen einer EA-Nummer, dann muß die Prüfziffer $a_{13} = 2$ sein, da

$$1{\cdot}9{+}3{\cdot}0{+}1{\cdot}0{+}3{\cdot}1{+}1{\cdot}3{+}3{\cdot}7{+}1{\cdot}5{+}3{\cdot}0{+}1{\cdot}0{+}3{\cdot}3{+}1{\cdot}7{+}3{\cdot}7{+}1{\cdot}2 = 80.$$

00–09:	USA, Kanada	76:	Schweiz
30–37:	Frankreich	80–81:	Italien
49:	Japan	87:	Niederlande
50:	Großbritannien	90–91:	Österreich

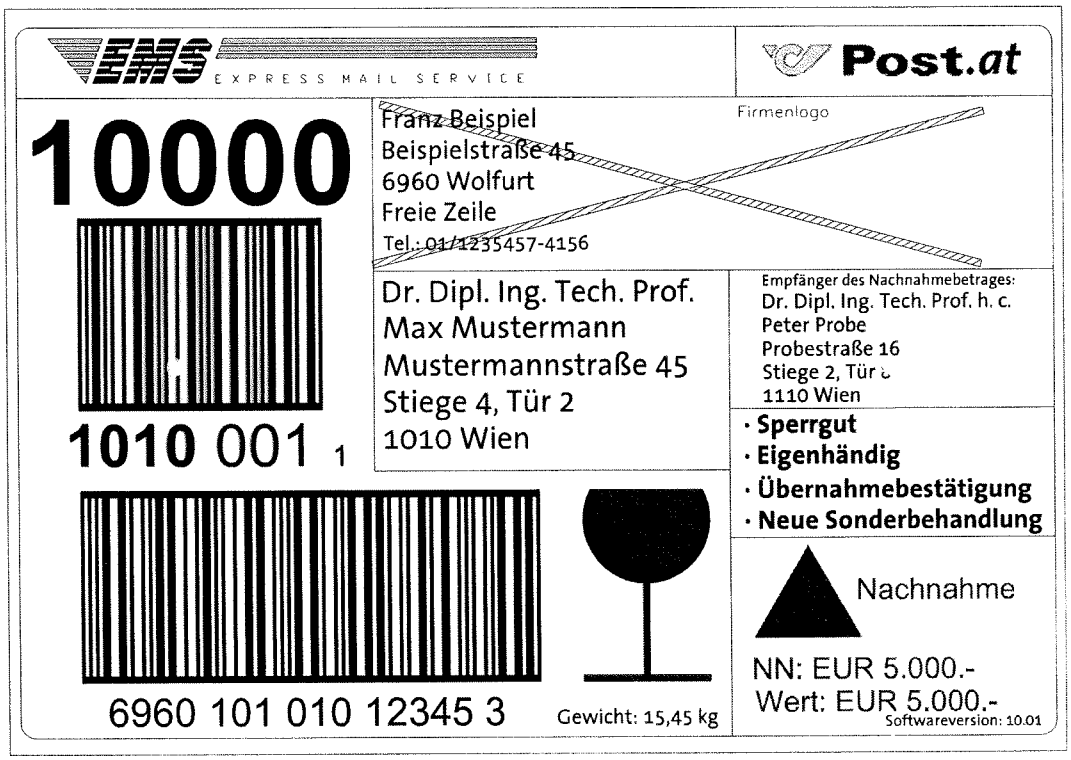
ENTDECKT: Einzelfehler

Phonetische Fehler

BEISPIEL FÜR EMS-LABEL (Zustellung bis 10:00 Uhr)

Das Feld für die Absenderadresse befindet sich im oberen Bereich,
rechts daneben wurde ein Platz für das Firmenlogo des Absenders reserviert.
Das Adressfeld des Empfängers befindet sich immer im unteren Bereich.
Anm.: Schwarz-Weiß-Ausdrucke sind ebenso gültig wie in Farbe.

Barcodedimensionen:
Breite schmaler Balken: 508um
Ratio= 1:2,25 => breiter Balken=1143um



Post.at	Verteilzentren/Technik		
EMS Querformat			
M-stab	1:1	Datum	28.01.03
		Bearbeiter	Mosbock
Blatt	1 von 9	Zeichner	Derkits, Post AG
Dateiname	Label.dwg		

Verschiedene Zahlendarstellungen

Dezimal	Binär	Binär Block	Hexadezimal
0	0	0000	0
1	1	0001	1
2	10	0010	2
3	11	0011	3
4	100	0100	4
5	101	0101	5
6	110	0110	6
7	111	0111	7
8	1000	1000	8
9	1001	1001	9
10	1010	1010	A
11	1011	1011	B
12	1100	1100	C
13	1101	1101	D
14	1110	1110	E
15	1111	1111	F

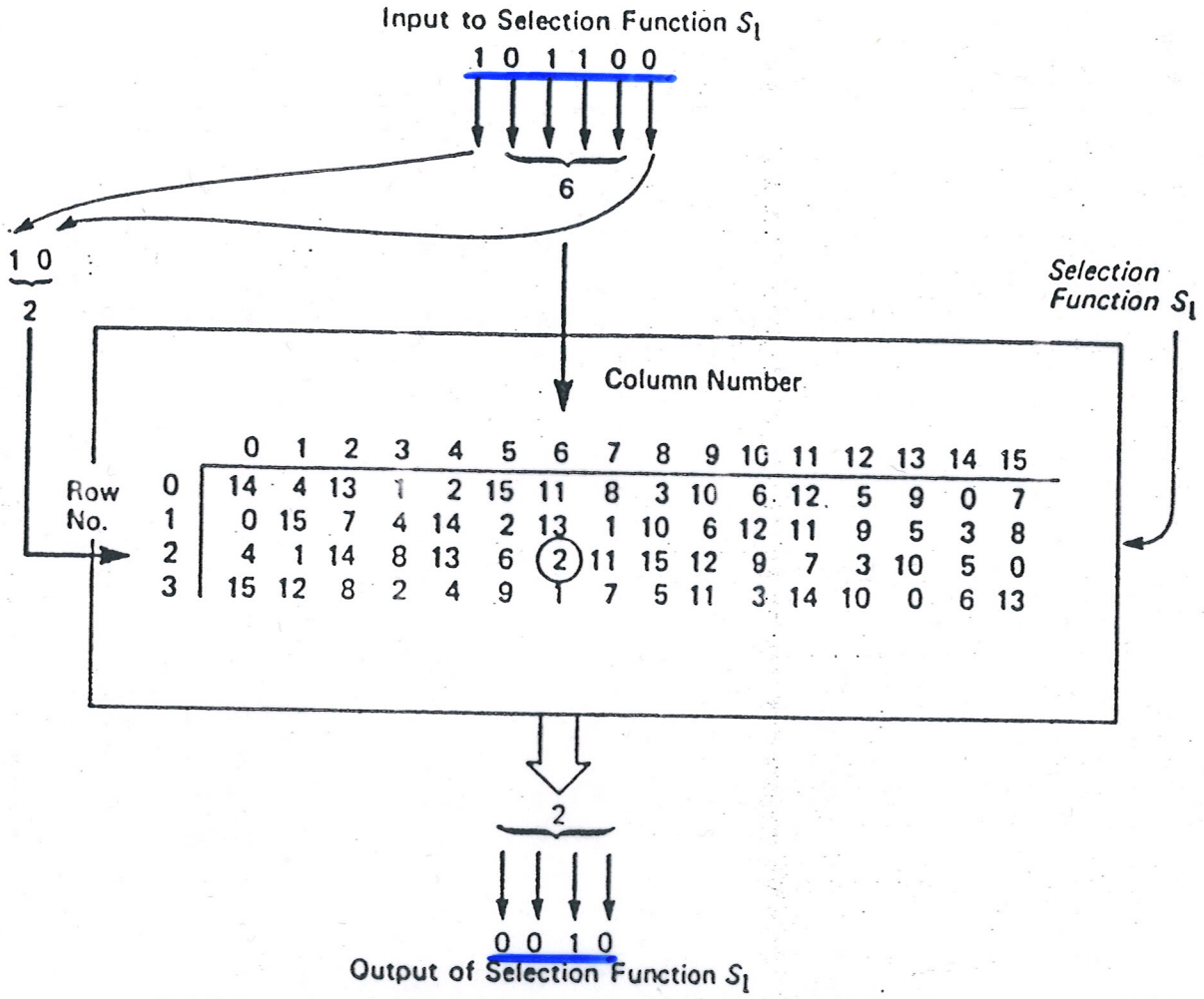


Figure . Example of the use of selection function S_1. Input is the 6-bit string 101100. Output is the 4-bit string 0010.

American Standard Code for Information Interchange (ASCII-Code)

Nummer im ASCII-Code	Zeichen	Binäres Wort o.Kontrollstelle	Binäres Wort mit Kontrollstelle
...	...	...	...
32	Zwischenraum	0100000	10100000
33	!	0100001	00100001
...	...	...	...
48	0	0110000	00110000
49	1	0110001	10110001
50	2	0110010	10110010
...	...	...	...
61	=	0111101	10111101
...	...	...	...
65	A	1000001	01000001
66	B	1000010	01000010
67	C	1000011	11000011
68	D	1000100	01000100
69	E	1000101	11000101
70	F	1000110	11000110
71	G	1000111	01000111
72	H	1001000	01001000
73	I	1001001	11001001
74	J	1001010	11001010
75	K	1001011	01001011
76	L	1001100	11001100
77	M	1001101	01001101
78	N	1001110	01001110
...	...	...	...
82	R	1010010	11010010
83	S	1010011	01010011
...	...	...	...
97	a	1100001	11100001
98	b	1100010	11100010
...	...	...	...
122	z	1111010	11111010
...	...	...	...
125	}	1111101	01111101
...	...	...	...

Demnach lautet z.B. die Darstellung des Textes "NEIN" mittels des ASCII-Codes:

$$\underset{\text{N}}{01001110}\ \underset{\text{E}}{11000101}\ \underset{\text{I}}{11001001}\ \underset{\text{N}}{01001110}$$

NEIN =

Moderne Verschlüsselungsverfahren

Vernam One-Time-Pad

(einziges nachweislich nicht knackbares Chiffriersystem)

Transformiere die Nachricht mit Hilfe des ASCII-Codes in eine Folge von Bits N.

Beide Kommunikationspartner besitzen die gleiche geheime binäre Zufallsfolge $S = 00110100\ 10110111\ 00111000\ 11010001\ 100\cdots$

Der Absender bildet $N \oplus_2 S = K$:

Nachricht "NEIN":	N	=	01001110	11000101	11001001	01001110
Binäre Zufallsfolge:	S	=	00110100	10110111	00111000	11010001	100$\cdots$
Kryptogramm:	K	=	01111010	01110010	11110001	10011111	

Der rechtmäßige Empfänger kennt S und bildet $K \oplus_2 S = N \oplus_2 S \oplus_2 S = N$:

Kryptogramm:	K	=	01111010	01110010	11110001	10011111	
Binäre Zufallsfolge:	S	=	00110100	10110111	00111000	11010001	100$\cdots$
Nachricht "NEIN":	N	=	01001110	11000101	11001001	01001110	

Auf dieses System bauen fast alle heutigen Chiffriersysteme auf. Man verwendet jedoch meistens zum Verschlüsseln keine Zufallsfolgen, sondern Pseudozufallsfolgen.

RSA Public-key Kryptosystem
(Rivest/Shamir/Adleman (1978))

Wähle zwei große Primzahlen p, q und berechne $p \cdot q = n$.

Suche ein e mit $ggT(e, (p-1)(q-1)) = 1$.

Ermittle ein d mit $e \cdot d \equiv 1 \mod (p-1)(q-1)$.

RSA Public-key Kryptosystem

Veröffentliche e und n.

Halte geheim p, q und d.

$M = C = \mathbb{Z}/(n) = \{0, 1, 2, ..., n-1\}$

Verschlüsselung: $E(m) = m^e \mod n = c, \ \forall m \in \mathbb{Z}/(n)$

Entschlüsselung: $D(c) = c^d \mod n = m, \ \forall c \in \mathbb{Z}/(n)$

Als Verschlüsselungs- und Entschlüsselungsfunktionen dienen spezielle Polynomfunktionen:

$x \to x^e$ ist eine Permutation von $\mathbb{Z}/(n)$,

$x \to x^d$ ist die zu $x \to x^e$ inverse Permutation von $\mathbb{Z}/(n)$.

Theorem Euler-Fermat:

$x^{e \cdot d} = x^{1+t \cdot (p-1)(q-1)} = x, \ \forall \ x \in \mathbb{Z}/(p \cdot q)$

Beispiel für den RSA-Verschlüsselungsalgorithmus

Wähle: $p = 5$, $q = 11$, dann folgt $m = 55$
Weiters sei $k = 3$, dann kann $s = 7$ gewählt werden.

Nachrichten: 0,1,2,3,4,5,6,$\cdots$, 53,54

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$x^3 \bmod 55$	0	1	8	27	9	15	51	13	17	14	10	11	23	52
x	14	15	16	17	18	19	20	21	22	23	24	25	26	27
$x^3 \bmod 55$	49	20	26	18	2	39	25	21	33	12	19	5	31	48
x	28	29	30	31	32	33	34	35	36	37	38	39	40	41
$x^3 \bmod 55$	7	24	50	36	43	22	34	30	16	53	37	29	35	6
x	42	43	44	45	46	47	48	49	50	51	52	53	54	
$x^3 \bmod 55$	3	32	44	45	41	38	42	4	40	46	28	47	54	

Klartext: 8

Verschlüsselung: $8^3 \bmod 55 = 512 \bmod 55 = 17$

Entschlüsselung: $17^7 \bmod 55 = 8$

Faktorisierungsproblem

Berechne

$59 \cdot 103 = 6077$

Finde

$6077 = p \cdot q$

Eine Methode, die Primteiler von 6077 zu finden ist zu probieren, welche der Primzahlen zwischen 2 und $\sqrt{6077} = 77,955\cdots$ die Zahl 6077 teilen. Man probiert also, welche der Primzahlen
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73
die Zahl 6077 teilen.

Es gibt aber bessere Verfahren die Primteiler von 6077 zu finden:
Methode von Fermat: $n = p \cdot q = s^2 - t^2, \;\; p = s - t, \;\; q = s + t$

$$\begin{aligned} 6077 &= s^2 - t^2 \\ &= 78^2 - 7 \\ &= 79^2 - 164 \\ &= 80^2 - 233 \\ &= 81^2 - 484 = 81^2 - 22^2 \end{aligned}$$

Damit gilt $6077 = 81^2 - 22^2$, daher $p = 81 - 22 = 59$ und $q = 81 + 22 = 103$.

Mit dieser Methode war es möglich, den 243 Dezimalstellen (807 Binärstellen) langen Modul der Bajuwarischen Befreiungsarmee im Bruchteil von Sekunden zu faktorisieren und damit die Verschlüsselung zu brechen.

Speichern von Passwörtern

Zur Konstruktion von Einwegfunktionen verwendet man üblicherweise schwierige mathematische Probleme.

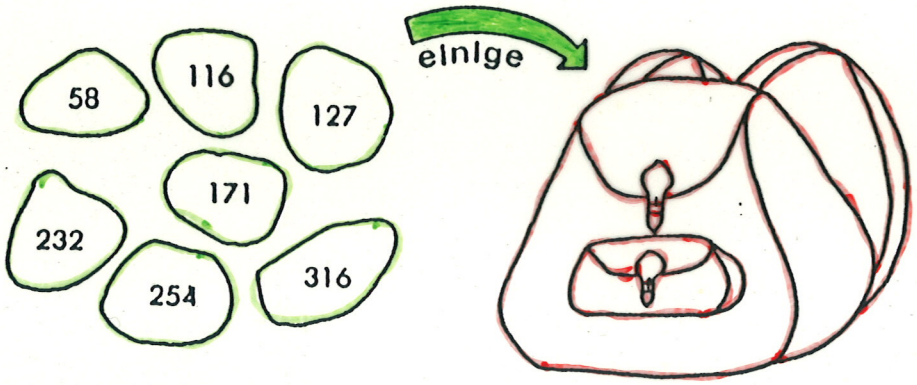
Beispiel: Teilsummenproblem - Rucksackproblem

$f: GF(2)^n \longrightarrow \mathbb{N}$

$f(b_1,\ldots,b_n) = (b_1,\ldots,b_n).(a_1,\ldots,a_n) = b_1a_1 + \ldots + b_na_n,$

wobei $(a_1,\ldots,a_n) \in \mathbb{N}^n$.

NP-vollständiges Problem, es gibt 2^n Lösungsmöglichkeiten



Gesamtgewicht: 1274 Rucksackgewicht: 846

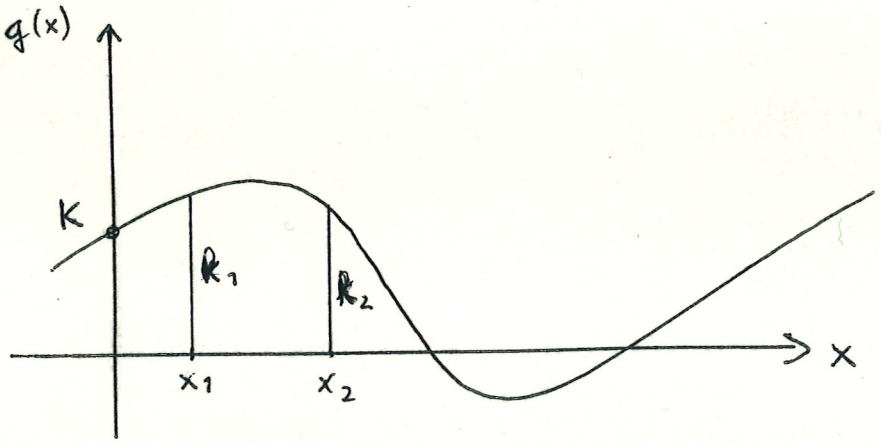
$(b_1,\ldots,b_7) = (0,0,1,1,1,0,1) \longrightarrow 846$

$0.58 + 0.116 + 1.127 + 1.171 + 1.232 + 0.254 + 1.316 = 846$

6.2 Threshold Schemes

Konstruktion und Verwaltung elektronischer Schlüssel mittels Polynominterpolation (A. Shamir (1979))

Ein Betrieb hat das folgende Problem: Man möchte n Teilschlüssel k_i $(1 \leq i \leq n)$ zu einem elektronischen Schloss ausgeben. Jede Teilmenge von $t \leq n$ Teilschlüssel k_i soll das Schloss öffnen. Weniger als t Teilschlüssel sollen ein "Aufsperren" nicht gestatten bzw. in absehbarer Zeit nicht gestatten.



Die Lösung dieses Problems erfolgt mittels der Intepolation nach *Lagrange*. Ist K der Generalschlüssel, welcher das Schloss sperrt (in der Praxis eine natürliche Zahl), so wählt man eine große Primzahl $p > K$ und $p > n$ und ein zufälliges Polynom vom Grad $t-1$:

$$g(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$$

über den Galoisfeld $GF(p)$ mit $a_0 = K$. Es gilt dann $g(0) = K$. Die Teilschlüssel k_i, $i = 1, 2, \cdots, t$ werden nun aus $g(x_i) = k_i$ berechnet. Damit

ist jedes Paar (x_i, k_i) ein Punkt auf $y = g(x)$. Da je t Punkte ein Polynom vom Grad $t-1$ eindeutig betimmen, kann $g(x)$ und damit $K = g(0)$ aus je t Teilschlüsseln berechnet werden. Aus weniger als t Teilschlüsseln ist dies bei genügend großem p in absehbarer Zeit jedoch nicht möglich.

Sind z.B. $k_1, k_2, \cdots, k_t$ gegeben, so erhält man $g(x)$ nach Lagrange als

$$g(x) = \sum_{s=1}^{t} k_s \prod_{j=1, j\neq s}^{k} \frac{x - x_j}{x_s - x_j} \bmod p$$

Beispiel: $k = 3, n = 5, p = 17, K = 13$

Man wählt ein zufälliges Polynom $g(x) = 2x^2 + 10x + 13 \bmod 17$, wobei allerdings $a_0 = 13$ sein muss.

$k_1 = g(1) = 2 + 10 + 13 \bmod 17 = 25 \bmod 17 = 8$
$k_2 = g(2) = 8 + 20 + 13 \bmod 17 = 41 \bmod 17 = 7$
$k_3 = g(3) = 18 + 30 + 13 \bmod 17 = 61 \bmod 17 = 10$
$k_4 = g(4) = 32 + 40 + 13 \bmod 17 = 85 \bmod 17 = 0$
$k_5 = g(5) = 50 + 50 + 13 \bmod 17 = 113 \bmod 17 = 11$

Somit sind die 5 verschiedenen Teilschlüssel gegeben durch $(1, 8), (2, 7), (3, 10), (4, 0), (5, 11)$.

Aus beliebigen 3 Teilschlüsseln, z.B. $(1, 8), (3, 10)$ und $(5, 11)$ kann $g(x)$ rekonstruiert werden:

$$g(x) = 8\frac{(x-3)(x-5)}{(1-3)(1-5)} + 10\frac{(x-1)(x-5)}{(3-1)(3-5)} + 11\frac{(x-1)(x-3)}{(5-1)(5-3)} \bmod 17$$

Beispiel: k=3, n=5, p=17, K=13

Wir wählen zufällig $g(x) = 2x^2 + 10x + 13 \ mod \ 17$

$K_1 = g(1) = 2 + 10 + 13 \ mod \ 17 = 25 \ mod \ 17 = 8$

$K_2 = g(2) = 8 + 20 + 13 \ mod \ 17 = 41 \ mod \ 17 = 7$

$K_3 = g(3) = 18 + 30 + 13 \ mod \ 17 = 61 \ mod \ 17 = 10$

$K_4 = g(4) = 32 + 40 + 13 \ mod \ 17 = 85 \ mod \ 17 = 0$

$K_5 = g(5) = 50 + 50 + 13 \ mod \ 17 = 113 \ mod \ 17 = 11$

Somit sind die 5 verschiedenen Teilschlüssel gegeben durch (1,8), (2,7), (3,10), (4,0), (5,11).

Aus beliebigen 3 Teilschlüsseln z.B. (1,8), (3,10) und (5,11) kann g(x) rekonstruiert werden:

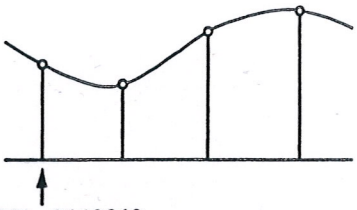
$$g(x) = 8\frac{(x-3)(x-5)}{(1-3)(1-5)} + 10\frac{(x-1)(x-5)}{(3-1)(3-5)} + 11\frac{(x-1)(x-3)}{(5-1)(5-3)} \ mod \ 17$$

Vorteile

- Man kann jederzeit zusätzlich Teilschlüssel ausgeben, ohne bereits ausgegebene Teilschlüssel ändern zu müssen.
- Bei Übergang zu einem neuen Polynom g(x) kann man einige der ausgegebenen Teilschlüssel behalten und andere vernichten.
- Die Einführung hierarchischer Systeme ist möglich, indem man an speziellen Personen mehrere Teilschlüssel gibt.

Compact Disk

Audiosignal:



Audioinformation: 10111001 , 0110010 , ...

Verfahren zur Fehlerkorrektur, Hinzufügen technischer Daten

Codierte Inf.: ... | 01100001 | 01000111 | ...

Kanalbits: 100001001000100000010010010010000 1

Lochmuster: