Was hat **Informatik** mit Sprache zu tun?

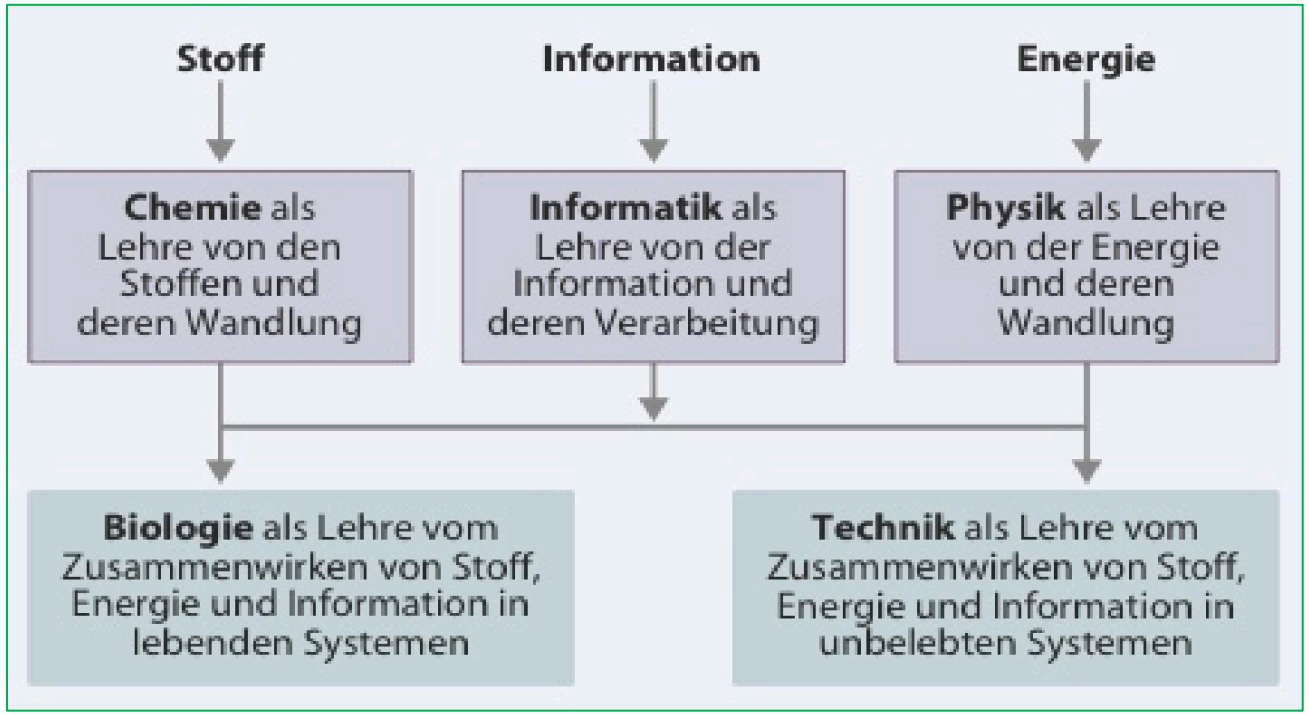
WILLKOMMEN
欢迎 स्वागत
BIENVENIDA
WELCOME
BIENVENUE ようこそ
добро пожаловать
ترحيب BEM-VINDO

Informatik als **Wissenschaft** der *strukturierten* und *automatisierten* Informationsverarbeitung.

Sprachen sind ein Mittel zur **Informationsübermittlung**, die Schrift zur **Informationsspeicherung** – beides hat viel mit Informatik zu tun.

*Wir unterscheiden **natürliche Sprachen** und **künstliche** (formale) **Sprachen**.*

Einleitung

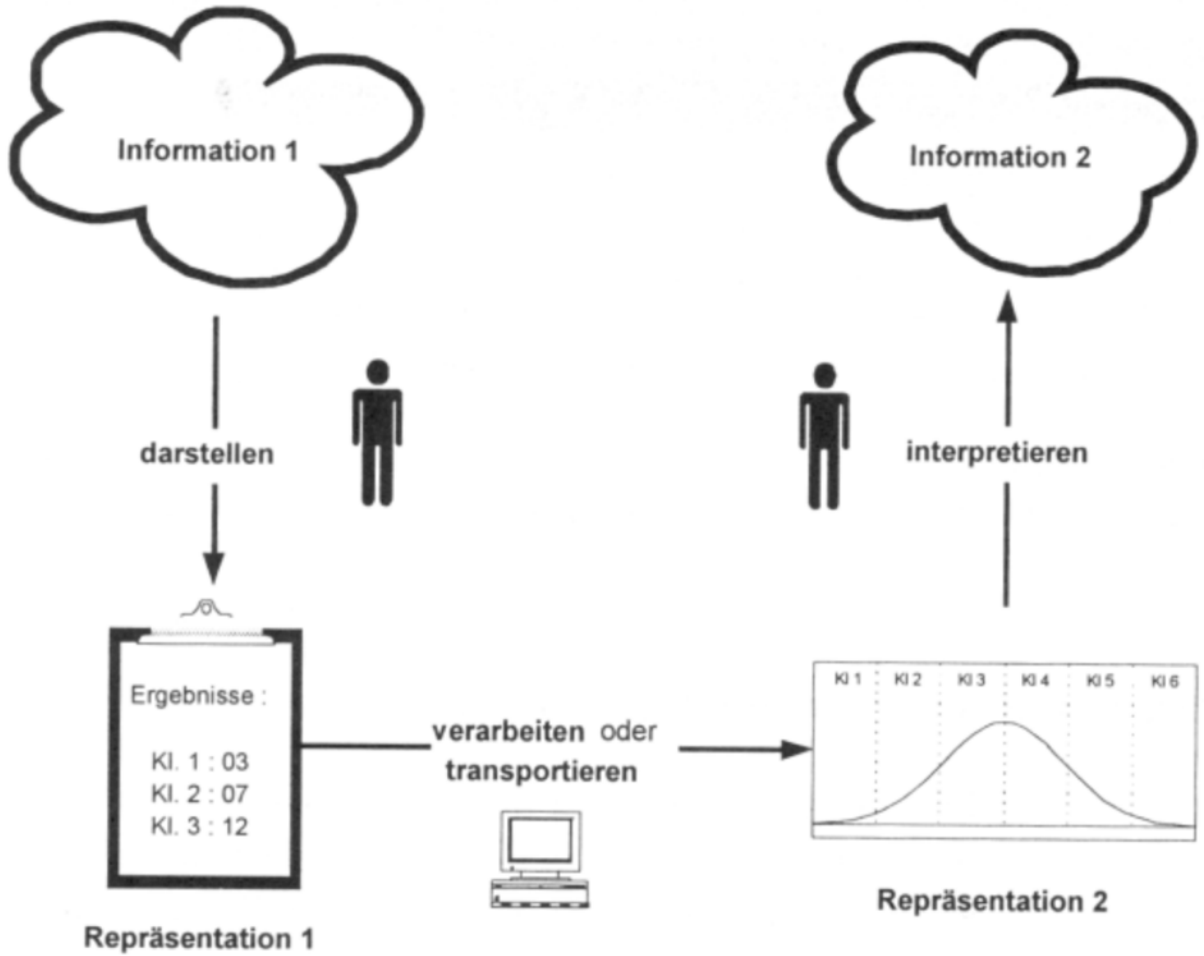


Norbert Breier: Informatik und die klassischen Naturwissenschaften (MNU Heft 3, 2006)

Sprecher des GI-Fachausschusses „Informatische Bildung in Schulen“

Einleitung

aus Hubwieser, Didaktik der Informatik, S.78:



Informatik und Schrift (Codes und Codierung)

Warum werden Emojis nicht überall gleich dargestellt?

Apple

Samsung

WhatsApp

Microsoft

Facebook

Schrift = Codierung von Information; Symbol ≙ Bedeutung

一 eins	中 innen, Mitte	花 Blume	力 Kraft	森 Wald
二 zwei	大 groß	草 Gras	気 Luft; Geist, Seele; Stimmung	正 richtig, gerecht
三 drei	小 klein	虫 Insekt	円 Yen; Kreis	水 Wasser
四 vier	月 Monat; Mond	犬 Hund	入 hineingehen	火 Feuer
五 fünf	日 Tag; Sonne	人 Person, Mensch	出 herauskommen	玉 Edelstein
六 sechs	年 Jahr	名 Name	立 aufstehen	王 König
七 sieben	早 früh; schnell	女 Frau	休 ausruhen	石 Stein
八 acht	木 Baum; Holz	男 Mann	先 vorher; vorne	竹 Bambus
九 neun	林 Hain, Forst	子 Kind	夕 Abend	糸 Faden
十 zehn	山 Berg	目 Auge	本 Buch; Ursprung	貝 Muschel
百 hundert	川 Fluss	耳 Ohr	文 Text	車 Fahrzeug
千 tausend	土 Erde	口 Mund	字 Schriftzeichen	金 Gold; Geld
上 oben	空 Himmel (vgl. *sky*)	手 Hand	学 lernen	雨 Regen
下 unten	田 Reisfeld	足 Fuß	校 Schule	赤 rot
左 links	天 Himmel (vgl. *heaven*)	見 sehen	村 Dorf	青 blau
右 rechts	生 Leben; roh	音 Ton, Geräusch	町 Stadt	白 weiß

Die Übertragung der Symbole der einen Darstellung von Information in die Symbole einer anderen Darstellung nennt man Codierung.

Die Zuordnungsvorschrift heisst **Code**.

Die Übertragung der Symbole der einen Darstellung von Information in die Symbole einer anderen Darstellung nennt man Codierung.

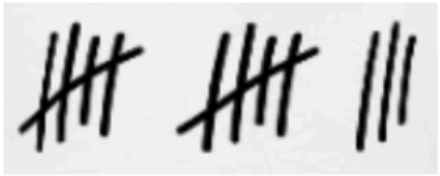
Die Zuordnungsvorschrift heisst **Code**.

Die Übertragung der Symbole der einen Darstellung von Information in die Symbole einer anderen Darstellung nennt man Codierung.

Die Zuordnungsvorschrift heisst **Code**.

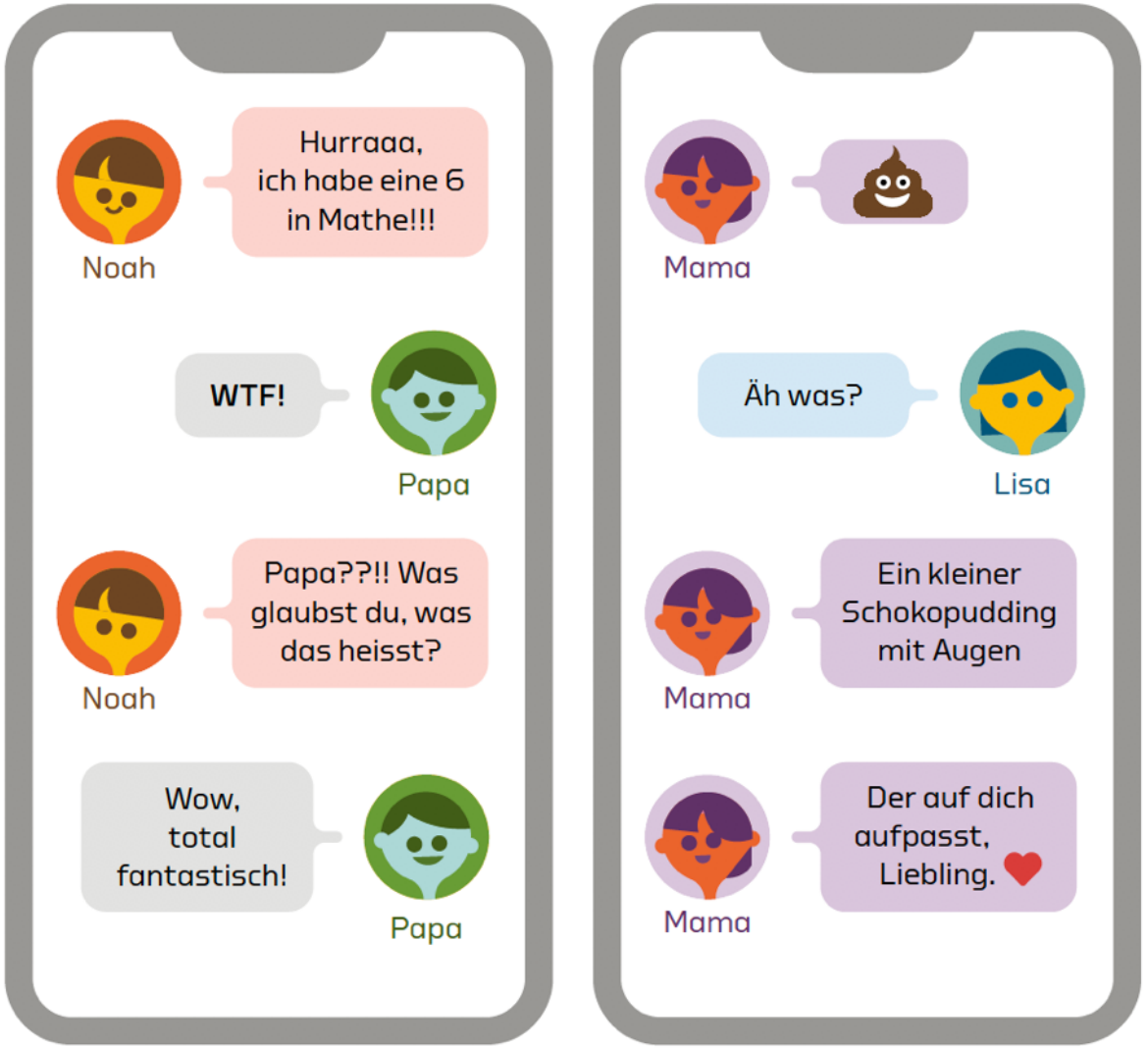
Die Übertragung der Symbole der einen Darstellung von Information in die Symbole einer anderen Darstellung nennt man Codierung.

Die Zuordnungsvorschrift heisst **Code**.

13  XIII   十三 ١٣

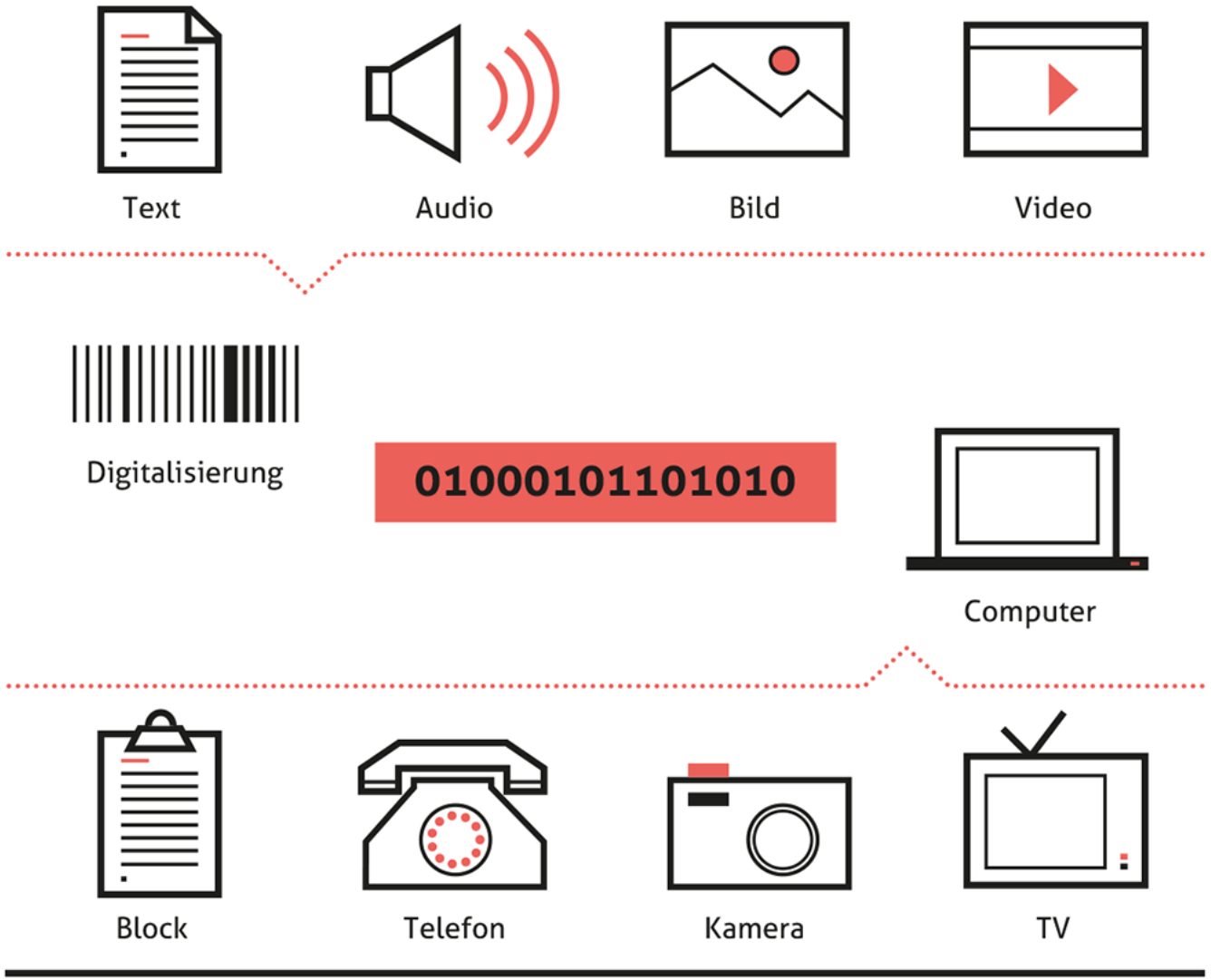
Decodieren ist gar nicht immer so einfach

Nanu?



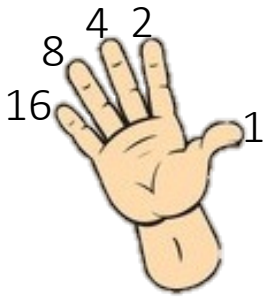
Connected 2, Seite 14

Digitalisierung: alles mit 0 und 1 aufschreiben können



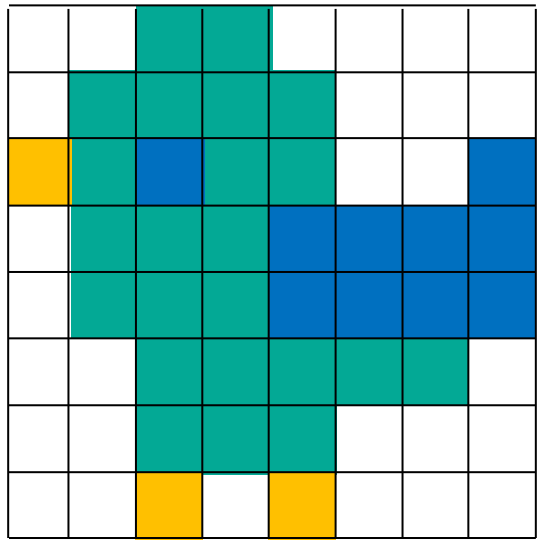
Digitalisierung: alles mit 0 und 1 aufschreiben können

9 = 1001



Zahlen

Bilder



ASCII-Code	Zeichen
00100000	Leerzeichen
01000001	A
01000010	B
01000011	C
01000100	D
01000101	E
01000110	F
01000111	G
01001000	H
01001001	I
01001010	J
01001011	K
01001100	L
...	...

Text

Ton

Video

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand eine Flasche vergiftet hat.

Sie haben 5 Ratten zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken.

Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von 10 Minuten.

In 20 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?

Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?

Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?

Rätsel-Tipp

Sie haben 30 Flaschen teuren Wein. Sie wissen, dass jemand eine Flasche vergiftet hat.

Sie haben 5 Ratten zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von 10 Minuten.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?





Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?

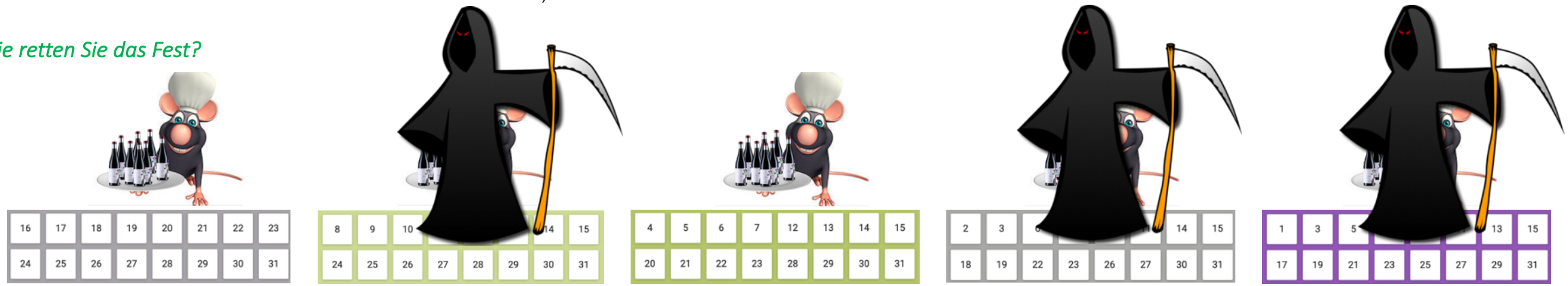
Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?



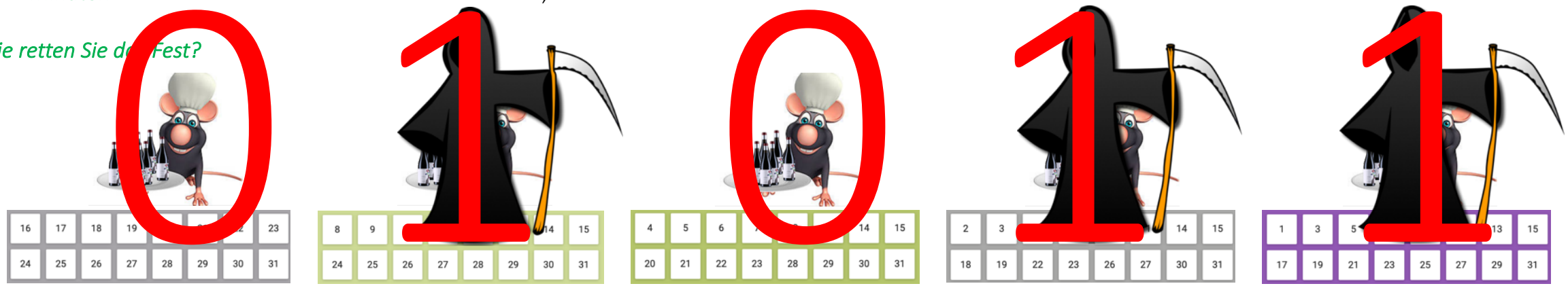
Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?



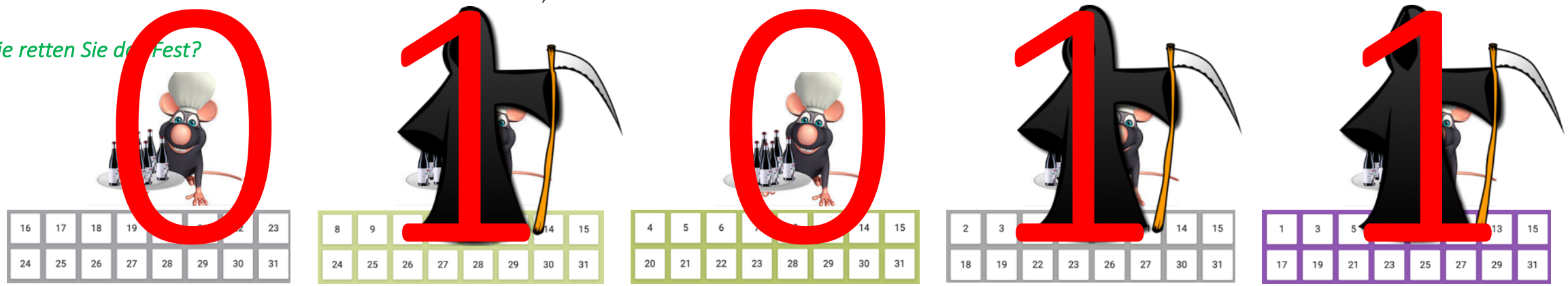
Rätsel-Tipp

Sie haben **30 Flaschen** teuren Wein. Sie wissen, dass jemand **eine Flasche** vergiftet hat.

Sie haben **5 Ratten** zur Verfügung. Jede von Ihnen kann beliebig viel Wein trinken. Trinkt eine Ratte vom vergifteten Wein, stirbt sie innerhalb von **10 Minuten**.

In 11 Minuten kommen ihre Gäste. Sie haben also keine Zeit, neuen Wein zu kaufen.

Wie retten Sie das Fest?



0 + 8 + 0 + 2 + 1 = Flasche 11

ASCII-Tabelle

Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex	Dec	Char	Bin	Hex
0	NULL	0000 0000	0	32		0010 0000	20	64	@	0100 0000	40	96	`	0110 0000	60	128	Ç	1000 0000	80	160	á	1010 0000	A0	192	└	1100 0000	C0	224	Ó	1110 0000	E0
1	SOH	0000 0001	1	33	!	0010 0001	21	65	A	0100 0001	41	97	a	0110 0001	61	129	ü	1000 0001	81	161	í	1010 0001	A1	193	┴	1100 0001	C1	225	ß	1110 0001	E1
2	STX	0000 0010	2	34	"	0010 0010	22	66	B	0100 0010	42	98	b	0110 0010	62	130	é	1000 0010	82	162	ó	1010 0010	A2	194	┬	1100 0010	C2	226	Ô	1110 0010	E2
3	ETX	0000 0011	3	35	#	0010 0011	23	67	C	0100 0011	43	99	c	0110 0011	63	131	â	1000 0011	83	163	ú	1010 0011	A3	195	├	1100 0011	C3	227	Ò	1110 0011	E3
4	EOT	0000 0100	4	36	$	0010 0100	24	68	D	0100 0100	44	100	d	0110 0100	64	132	ä	1000 0100	84	164	ñ	1010 0100	A4	196	─	1100 0100	C4	228	õ	1110 0100	E4
5	ENQ	0000 0101	5	37	%	0010 0101	25	69	E	0100 0101	45	101	e	0110 0101	65	133	à	1000 0101	85	165	Ñ	1010 0101	A5	197	┼	1100 0101	C5	229	Õ	1110 0101	E5
6	ACK	0000 0110	6	38	&	0010 0110	26	70	F	0100 0110	46	102	f	0110 0110	66	134	å	1000 0110	86	166	ª	1010 0110	A6	198	ã	1100 0110	C6	230	µ	1110 0110	E6
7	BEL	0000 0111	7	39	'	0010 0111	27	71	G	0100 0111	47	103	g	0110 0111	67	135	ç	1000 0111	87	167	º	1010 0111	A7	199	Ã	1100 0111	C7	231	þ	1110 0111	E7
8	BS	0000 1000	8	40	(	0010 1000	28	72	H	0100 1000	48	104	h	0110 1000	68	136	ê	1000 1000	88	168	¿	1010 1000	A8	200	╚	1100 1000	C8	232	Þ	1110 1000	E8
9	HT	0000 1001	9	41	)	0010 1001	29	73	I	0100 1001	49	105	i	0110 1001	69	137	ë	1000 1001	89	169	®	1010 1001	A9	201	╔	1100 1001	C9	233	Ú	1110 1001	E9
10	LF	0000 1010	A	42	*	0010 1010	2A	74	J	0100 1010	4A	106	j	0110 1010	6A	138	è	1000 1010	8A	170	¬	1010 1010	AA	202	╩	1100 1010	CA	234	Û	1110 1010	EA
11	VT	0000 1011	B	43	+	0010 1011	2B	75	K	0100 1011	4B	107	k	0110 1011	6B	139	ï	1000 1011	8B	171	½	1010 1011	AB	203	╦	1100 1011	CB	235	Ù	1110 1011	EB
12	FF	0000 1100	C	44	,	0010 1100	2C	76	L	0100 1100	4C	108	l	0110 1100	6C	140	î	1000 1100	8C	172	¼	1010 1100	AC	204	╠	1100 1100	CC	236	ý	1110 1100	EC
13	CR	0000 1101	D	45	-	0010 1101	2D	77	M	0100 1101	4D	109	m	0110 1101	6D	141	ì	1000 1101	8D	173	¡	1010 1101	AD	205	═	1100 1101	CD	237	Ý	1110 1101	ED
14	SO	0000 1110	E	46	.	0010 1110	2E	78	N	0100 1110	4E	110	n	0110 1110	6E	142	Ä	1000 1110	8E	174	«	1010 1110	AE	206	╬	1100 1110	CE	238	¯	1110 1110	EE
15	SI	0000 1111	F	47	/	0010 1111	2F	79	O	0100 1111	4F	111	o	0110 1111	6F	143	Å	1000 1111	8F	175	»	1010 1111	AF	207	¤	1100 1111	CF	239	´	1110 1111	EF
16	DLE	0001 0000	10	48	0	0011 0000	30	80	P	0101 0000	50	112	p	0111 0000	70	144	É	1001 0000	90	176	░	1011 0000	B0	208	ð	1101 0000	D0	240	-	1111 0000	F0
17	DC1	0001 0001	11	49	1	0011 0001	31	81	Q	0101 0001	51	113	q	0111 0001	71	145	æ	1001 0001	91	177	▒	1011 0001	B1	209	Ð	1101 0001	D1	241	±	1111 0001	F1
18	DC2	0001 0010	12	50	2	0011 0010	32	82	R	0101 0010	52	114	r	0111 0010	72	146	Æ	1001 0010	92	178	▓	1011 0010	B2	210	Ê	1101 0010	D2	242	‗	1111 0010	F2
19	DC3	0001 0011	13	51	3	0011 0011	33	83	S	0101 0011	53	115	s	0111 0011	73	147	ô	1001 0011	93	179	│	1011 0011	B3	211	Ë	1101 0011	D3	243	¾	1111 0011	F3
20	DC4	0001 0100	14	52	4	0011 0100	34	84	T	0101 0100	54	116	t	0111 0100	74	148	ö	1001 0100	94	180	┤	1011 0100	B4	212	È	1101 0100	D4	244	¶	1111 0100	F4
21	NAK	0001 0101	15	53	5	0011 0101	35	85	U	0101 0101	55	117	u	0111 0101	75	149	ò	1001 0101	95	181	Á	1011 0101	B5	213	ı	1101 0101	D5	245	§	1111 0101	F5
22	SYN	0001 0110	16	54	6	0011 0110	36	86	V	0101 0110	56	118	v	0111 0110	76	150	û	1001 0110	96	182	Â	1011 0110	B6	214	Í	1101 0110	D6	246	÷	1111 0110	F6
23	ETB	0001 0111	17	55	7	0011 0111	37	87	W	0101 0111	57	119	w	0111 0111	77	151	ù	1001 0111	97	183	À	1011 0111	B7	215	Î	1101 0111	D7	247	¸	1111 0111	F7
24	CAN	0001 1000	18	56	8	0011 1000	38	88	X	0101 1000	58	120	x	0111 1000	78	152	ÿ	1001 1000	98	184	©	1011 1000	B8	216	Ï	1101 1000	D8	248	°	1111 1000	F8
25	EM	0001 1001	19	57	9	0011 1001	39	89	Y	0101 1001	59	121	y	0111 1001	79	153	Ö	1001 1001	99	185	╣	1011 1001	B9	217	┘	1101 1001	D9	249	¨	1111 1001	F9
26	SUB	0001 1010	1A	58	:	0011 1010	3A	90	Z	0101 1010	5A	122	z	0111 1010	7A	154	Ü	1001 1010	9A	186	║	1011 1010	BA	218	┌	1101 1010	DA	250	·	1111 1010	FA
27	ESC	0001 1011	1B	59	;	0011 1011	3B	91	[	0101 1011	5B	123	{	0111 1011	7B	155	ø	1001 1011	9B	187	╗	1011 1011	BB	219	█	1101 1011	DB	251	¹	1111 1011	FB
28	FS	0001 1100	1C	60	<	0011 1100	3C	92	\	0101 1100	5C	124	|	0111 1100	7C	156	£	1001 1100	9C	188	╝	1011 1100	BC	220	▄	1101 1100	DC	252	³	1111 1100	FC
29	GS	0001 1101	1D	61	=	0011 1101	3D	93	]	0101 1101	5D	125	}	0111 1101	7D	157	Ø	1001 1101	9D	189	¢	1011 1101	BD	221	¦	1101 1101	DD	253	²	1111 1101	FD
30	RS	0001 1110	1E	62	>	0011 1110	3E	94	^	0101 1110	5E	126	~	0111 1110	7E	158	×	1001 1110	9E	190	¥	1011 1110	BE	222	▌	1101 1110	DE	254	■	1111 1110	FE
31	US	0001 1111	1F	63	?	0011 1111	3F	95	_	0101 1111	5F	127	DEL	0111 1111	7F	159	ƒ	1001 1111	9F	191	┐	1011 1111	BF	223	▀	1101 1111	DF	255	nbsp	1111 1111	FF

Markus schenkt seiner Frau eine Perlenkette.

Wie heisst seine Frau?

Zurück zu den Emojis

fehlererkennende vs fehlerkorrigierende Codes

EAN (Europäische Artikel Nummer)

ISBN (International Standard Book Number)

978-3-8348-0774-8

fehlererkennende vs fehlerkorrigierende Codes

Zaubertrick

Informatik ohne Strom - Datenstrukturen

Zaubertrick - Fehlerkorrektur

phsz

6

Worum geht es?

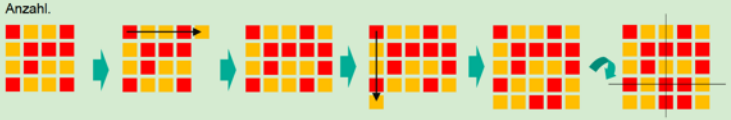
Du lernst einen verblüffenden Zaubertrick kennen, der nur 25 Karten (z.B. Spielkarten oder Postkarten) benötigt.
Gleichzeitig lernst du das Prinzip kennen, wie Computer Fehler beim Eintippen, Einlesen oder Übertragen von Daten erkennen oder gar korrigieren können.

Wie funktioniert es?

1. Der Zaubertrick

Du benötigst 25 gleich grosse Karten mit deutlich unterscheidbaren Vorder- und Rückseiten (hell / dunkel). Lasse jemanden aus dem Publikum aus 16 Karten ein quadratisches Muster mit 4 x 4 Karten auflegen. Dabei sollen sich Vorder- und Rückseite möglichst zufällig abwechseln, so dass das entstehende Muster schwer zu merken ist.

Nun behauptest du, dass du die Sache noch etwas schwieriger machen möchtest und legst noch eine weitere Spalte rechts dazu. Du tust so, als seien diese zusätzlichen Karten ganz zufällig. In Wirklichkeit zählst du schnell in jeder Zeile die Anzahl Karten mit dunkler Seite. Ist die Anzahl gerade, legst du die zusätzliche Karte mit der hellen Seite daneben, sonst mit der dunklen Seite. (Würdest du nach dem Legen der fünften Karte nochmals zählen, musst du eine gerade Anzahl dunkler Karten haben). Das Gleiche machst du anschliessend mit den Spalten, um insgesamt 5 x 5 Karten aufzulegen. Diesmal zählst du von oben nach unten die Anzahl dunkler Karten und ergänzt wieder zu einer geraden Anzahl.



Bitte nun jemanden aus dem Publikum **genau eine** der 25 Karten umzudrehen (hell/dunkel), ohne dass du es sehen kannst. Danach schaust du kurz auf das Spielfeld, um sogleich auf magische Weise auf die Karte zu zeigen, die gedreht wurde. Woher wusstest du, welche es war? Dazu zählst du erneut in jeder Zeile und jeder Spalte die dunklen Karten zusammen. Es wird jetzt genau eine Zeile und eine Spalte mit einer *ungeraden* Anzahl dunkler Karten geben. Dort wo sich diese Zeile und diese Spalte kreuzen, wurde die Karte gedreht. (Ist das nicht der Fall, hat die Person aus dem Publikum beim Umdrehen gemogelt. Sie hat entweder mehrere Karten oder gar keine Karte gedreht.)
Übrigens: Du kannst auch mehr Karten verwenden und zum Beispiel mit 5x5 Karten beginnen – das Prinzip bleibt immer gleich. Probiere den Trick mit deinen Eltern oder Geschwistern aus und lasse sie raten, wie er funktioniert ☺

2. Die Idee der Redundanz und Prüfsumme

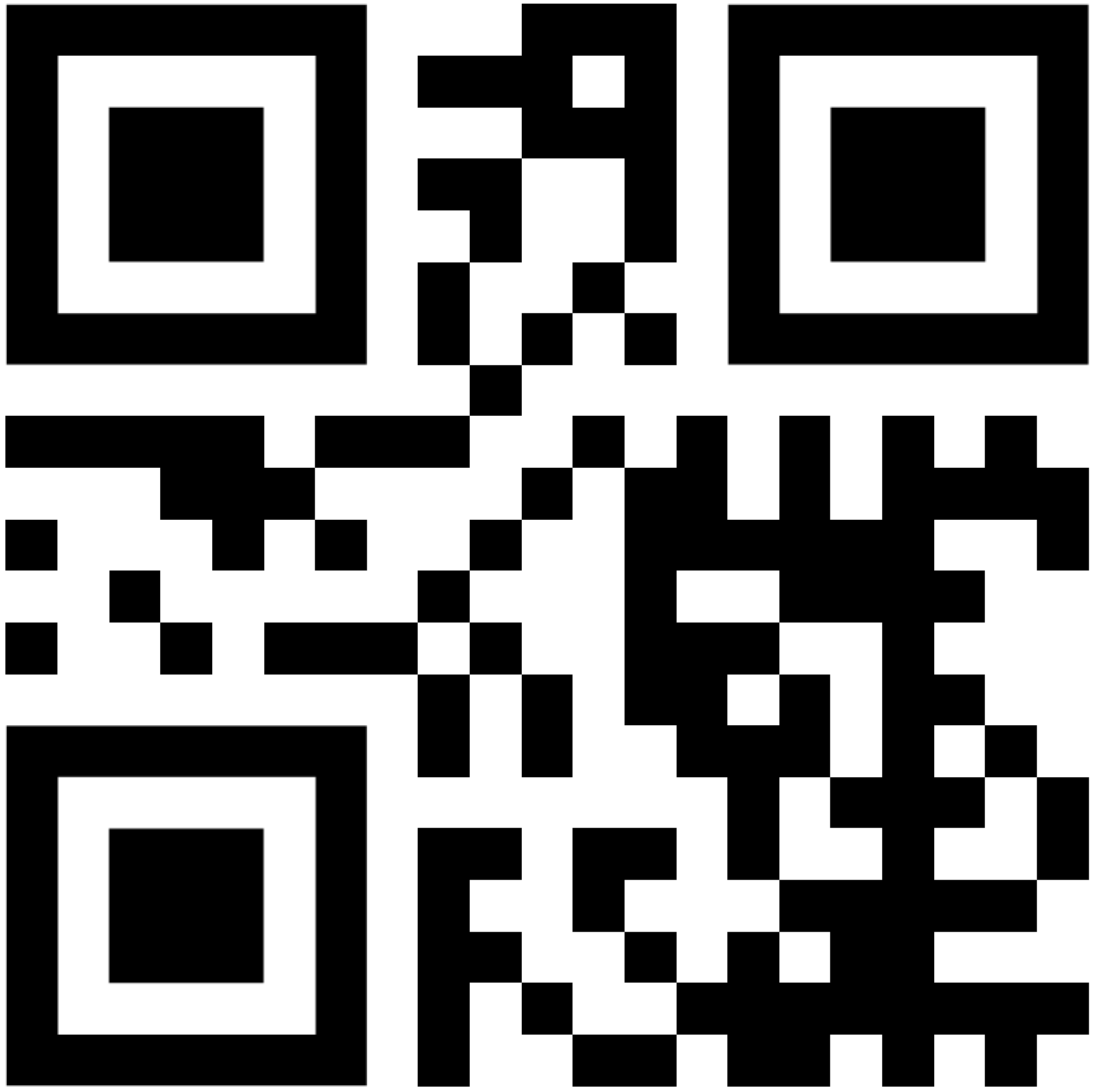
In der Informatik wird dieses Prinzip als **Redundanz** bezeichnet. Die zusätzliche Zeile und Spalte benötigen wir nur, um Fehler zu finden, sie sind aber nicht Teil der eigentlichen Information. Je nach Verfahren lassen sich Fehler sogar automatisch korrigieren, wie im Beispiel des Zaubertricks. Wusstest du, dass etwas 33% aller Daten auf einer CD nur zur Fehlererkennung und Fehlerkorrektur genutzt werden? Damit lässt sich eine CD trotz leichter Kratzer immer noch ohne Störgeräusche abspielen.
Es gibt auch sonst überall redundante Daten im Alltag. Ein weiteres Beispiel sind **Prüfsummen**. Sie werden im Supermarkt beim Einscannen vonBarcodes, bei ISBN-Nummern auf Büchern oder bei der Seriennummer von Geldscheinen verwendet. Auch Bankkontonummern enthalten Prüfziffern, damit bei einem Tippfehler nicht so leicht falsche Überweisungen passieren.

Wo wurde hier jeweils eine Karte gedreht?

EAN (Europäische Artikel Nummer)

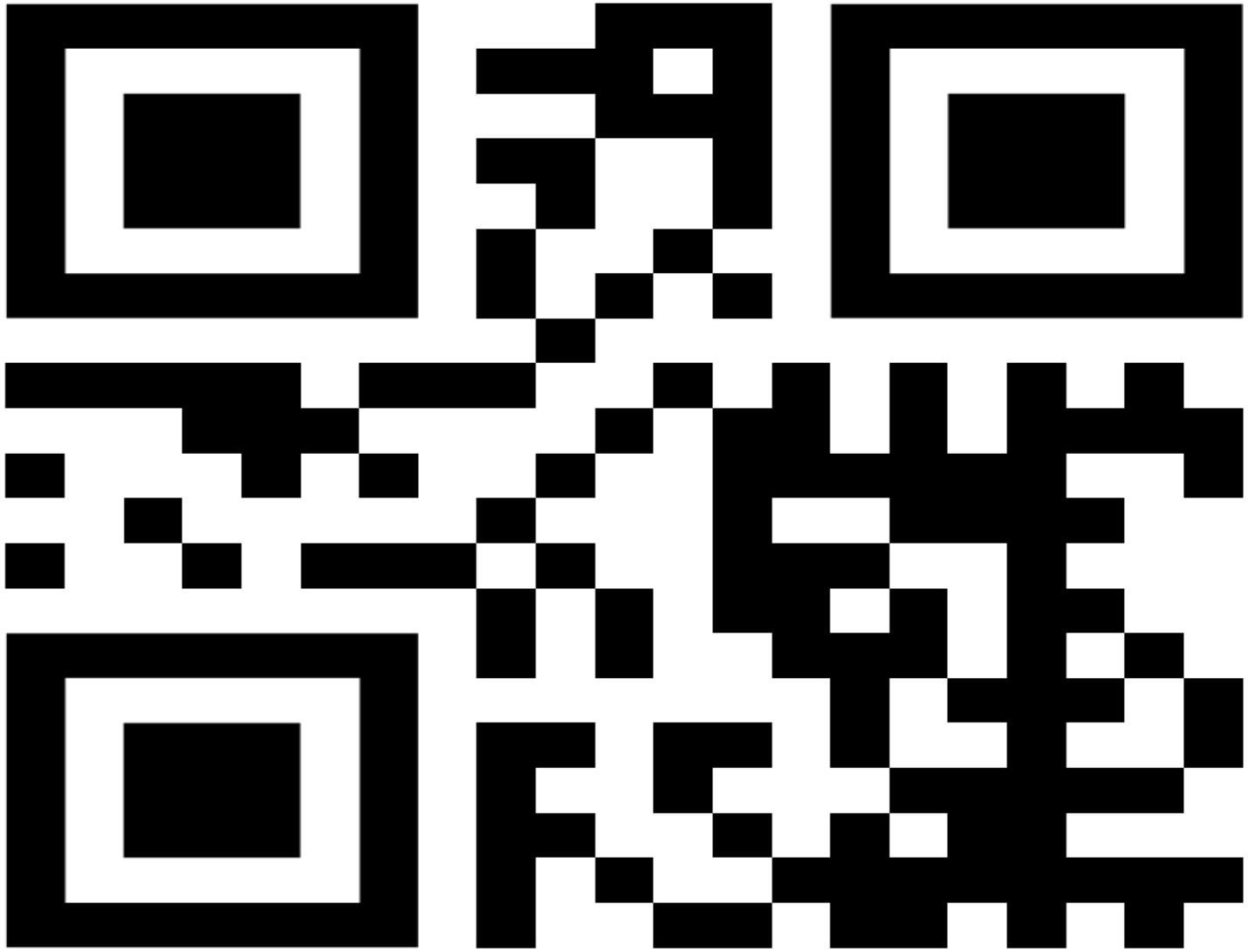
Nutzziffern	5 0 3 8 8 6 2 3 6 6 5 0
Multiplikatoren	1 3 1 3 1 3 1 3 1 3 1 3
Ergebnis	5 + 0 + 3 + 24 + 8 + 18 + 2 + 9 + 6 + 18 + 5 + 0 = **98**
Prüfziffer	Differenz zum nächsten Vielfachen von 10 = 2
EAN-Code	5 0 3 8 8 6 2 3 6 6 5 0 2

QR-Code (Quick Response)

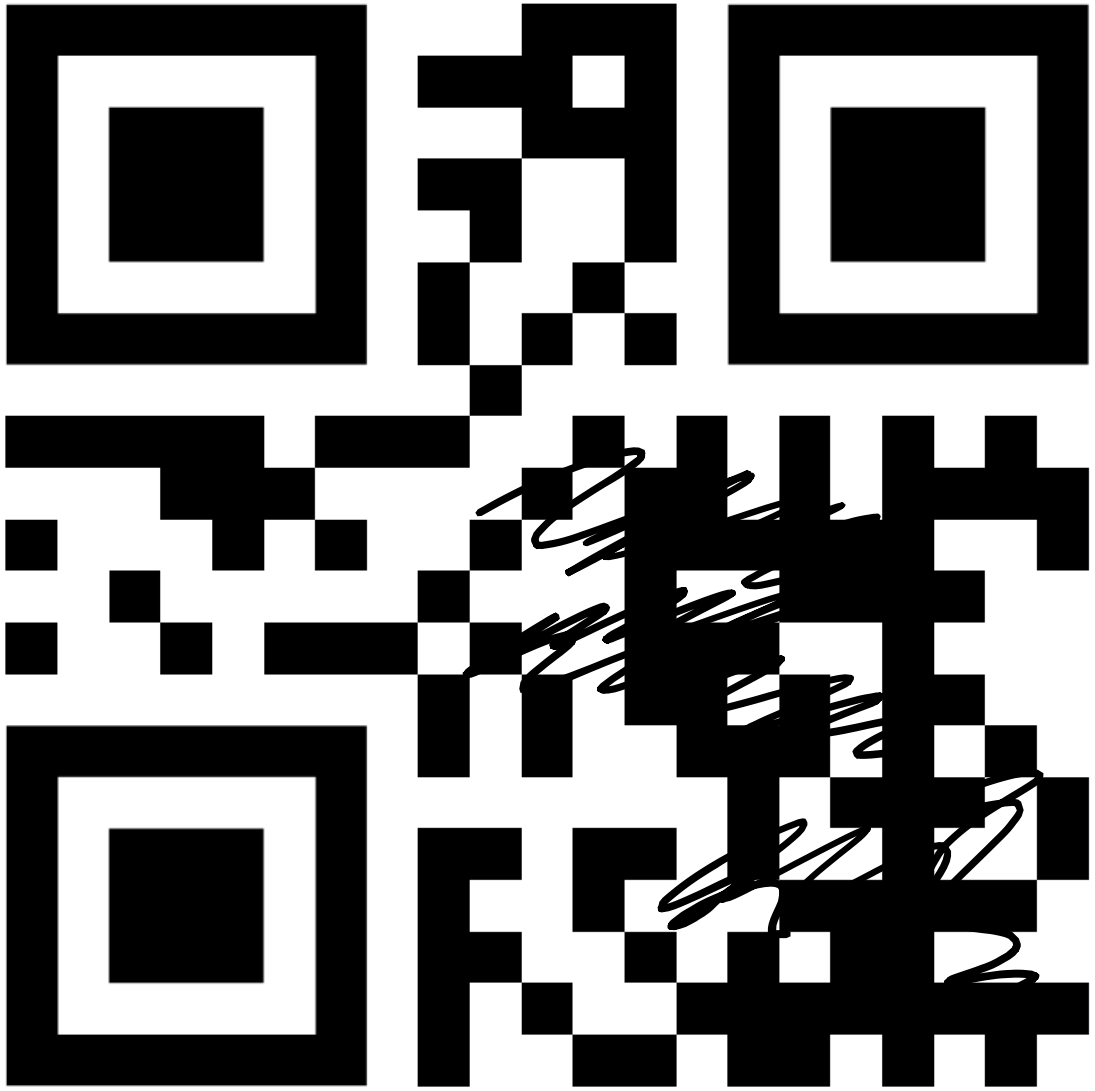


QR-Code (Quick Response)

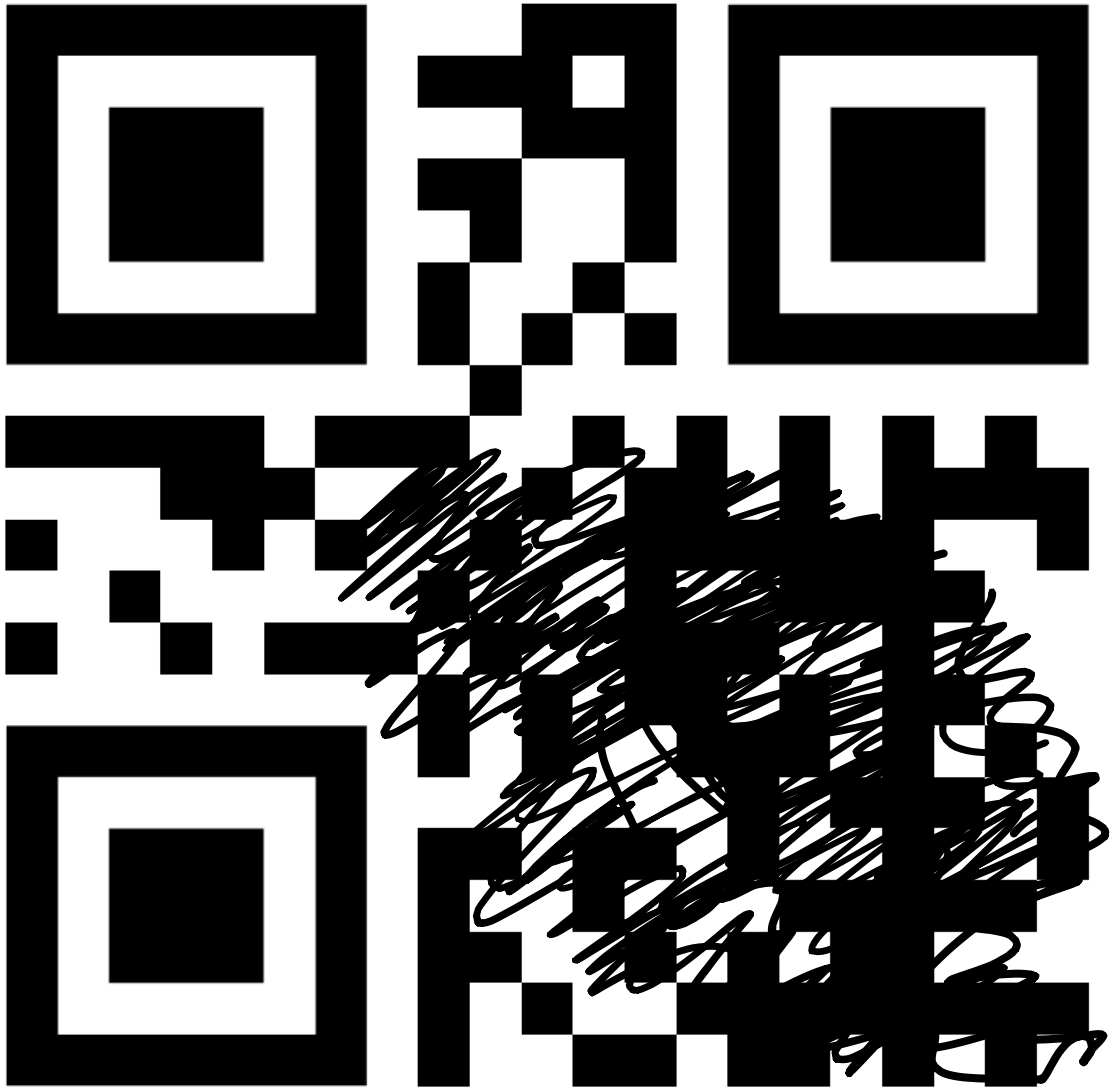
QR-Code (Quick Response)



QR-Code (Quick Response)



QR-Code (Quick Response)



QR- Codes haben verschiedene Fehlerkorrekturlevels

Bei Level H z.B. kann bis zu 30% des Codes verschmutzt oder überschrieben sein

fehlererkennende vs fehlerkorrigierende Codes

Der kleine Nick möchte an der Information abgeholt werden ... Ich wiederhole: Der kleine Nick möchte an der Information abgeholt werden!

Der Fahrer mit dem Kennzeichen ZH 12345 soll sich zu seinem Fahrzeug begeben ... Ich wiederhole: Der Fahrer mit dem Kennzeichen ZH 12345 soll sich zu seinem Fahrzeug begeben!

fehlererkennende vs fehlerkorrigierende Codes

Findest du heraus, welches Wort Cassini hier zur Erde gefunkt hat?

RRKRRROLOO7OTTTTTTTA3AAAATTTBTTIIIIIIOOO9OONZNN&N

Hamming-Code - Wikipedia

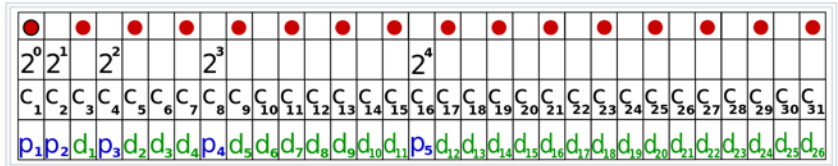
Berechnung der Paritätsstellen [Bearbeiten | Quelltext bearbeiten]

Die k Paritätsstellen (Kontrollbits) in einem Codewort werden nach einem Verfahren berechnet, wie es auch bei dem einfachen Paritäts-Prüfbit zur Anwendung kommt. Im Regelfall wird vereinbarungsgemäß eine gerade Parität für alle Kontrollstellen gewählt: Ist die Anzahl der logischen-1 der in die jeweilige Kontrollstelle eingerechneten Datenbitstellen eine gerade Anzahl, ist das jeweilige Paritätsbit logisch-0. Ist die Anzahl der logisch-1 in den Datenbitstellen eine ungerade Anzahl, wird das jeweilige Paritätsbit auf logisch-1 gesetzt, so dass sich in Summe in den Datenbitstellen und den Paritätsbit, immer eine gerade Anzahl von logisch-1 Bits ergibt.

Die einzelnen Paritätsbits eines Codewortes werden nicht über alle Stellen (Bits) des Datenwortes gebildet, sondern nur über einzelne, ausgewählte Datenbits. Zur Konstruktion, welche Datenbitstellen in welche Kontrollbits eingerechnet werden, kann nach einer anschaulichen Methode vorgegangen werden. Zunächst wird dazu der Rahmen des Codewortes aus den Datenbits und den Kontrollstellen gebildet:

1. Im Codewort befinden sich an denjenigen Positionen, die Zweierpotenzen sind (1, 2, 4, 8, 16, …), die einzelnen Paritäts-Kontrollbits p.
2. Die Datenbits d des zu übertragenden Datenwortes werden dazwischen auf den freien Stellen im Codewort von links aufsteigend eingetragen.

Sind $p_1, p_2, \ldots, p_k$ Paritätsbits, $d_1, d_2, \ldots, d_{N-k}$ Bits des Datenwortes und $c_1, c_2, \ldots, c_N$ die Bits des zu bildenden Codewortes, hat ein Codewort des so konstruierten Hamming-Code die folgende Form (diese Darstellung kann für größere Codewortlängen entsprechend erweitert werden):



Anordnung der Paritäts-Kontrollstellen $p_1 \ldots p_k$ und der Datenbits $d_1 \ldots d_{N-k}$ in einem Codewort mit den Stellen $c_1 \ldots c_N$ für die im Folgenden dargestellte Bitanordnung.

In das erste Paritätsbit p_1 werden nur jene Datenbits einbezogen, welche um eine Bitstelle weiter rechts im Codewort stehen und ein Bit als Datenbreite umfassen. Für das erste Paritätsbit ergeben sich als Folge von Codewortstellen somit alle Datenbits, die an ungerade Position im Codewort stehen:

$$c_1 = p_1 = c_3 \oplus c_5 \oplus c_7 \oplus c_9 \oplus c_{11} \oplus c_{13} \oplus c_{15} \oplus c_{17} \oplus c_{19} \oplus \cdots$$

Das Symbol $\oplus$ ist die logische XOR-Funktion und stellt zugleich die Bildungsvorschrift für die Kontrollbits dar. Wie weiter mit Hilfe obiger Tabelle zu erkennen ist, kommen an den angeführten Bitpositionen im Codewort auf der rechten Seite der Gleichung nur Datenbits vor. Dies gilt für alle Paritätsbits.

In das zweite Paritätsbit p_2 wird das rechts von p_2 im Codewort stehende Bit c_3 einberechnet, dann zwei Stellen im Codewort übersprungen, die nächsten zwei Bit c_6 und c_7 einberechnet, wieder zwei Stellen übersprungen, und so weiter. Statt eines Datenbits werden also zwei benachbarte Datenbits genommen und im Codewort zwei Stellen übersprungen. Damit ergibt sich für p_2 die Bildungsvorschrift:

$$c_2 = p_2 = c_3 \oplus c_6 \oplus c_7 \oplus c_{10} \oplus c_{11} \oplus c_{14} \oplus c_{15} \oplus c_{18} \oplus c_{19} \oplus \cdots$$

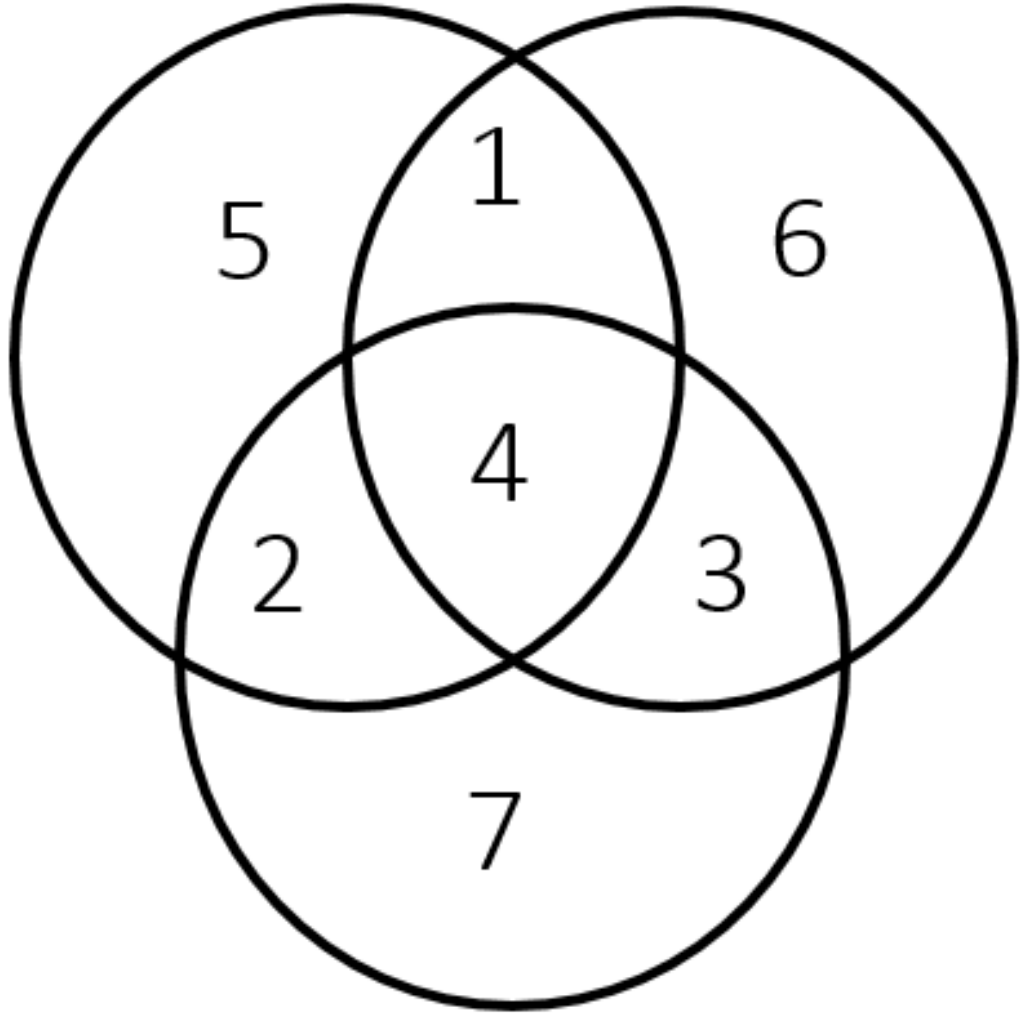
In das dritte Paritätsbit p_3 werden die rechts im Codewort folgenden drei Stellen einberechnet, es werden vier Stellen des Codewortes übersprungen, dann vier Bit einberechnet, dann vier Stellen übersprungen, und so weiter. Es werden also Gruppen zu je vier Bits für die Bildung des Paritätsbits herangezogen. Damit ergibt sich für p_3 :

$$c_4 = p_3 = c_5 \oplus c_6 \oplus c_7 \oplus c_{12} \oplus c_{13} \oplus c_{14} \oplus c_{15} \oplus c_{20} \oplus \cdots$$

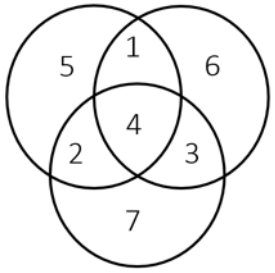
Das Paritätsbit p_i wird also über alle Stellen c_j des Codeworts berechnet, in denen an der i-ten Stelle der Binärkodierung des Index j eine logische Eins steht. Nach diesem Verfahren wird für die restlichen Paritätsbits analog fortgefahren, bis alle Paritätsbits des gewählten Hamming-Code bestimmt sind. Das Bestimmen des Codeworts wird in praktischen Applikationen durch den sogenannten *Encoder* vorgenommen.

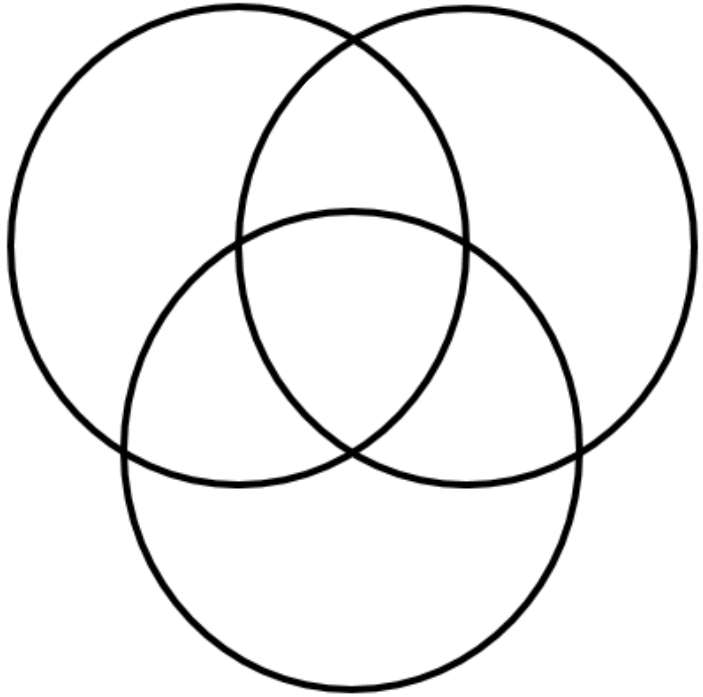
Hamming-Code (konkret: 4 Datenbits – 3 Prüfbits)

- Er trägt 4 Datenbits (1 bis 4) und 3 Prüfbits (5 bis 7).
- Die Prüfbits werden so gewählt, dass die Summe der Zahlen in jedem Kreis gerade ist.

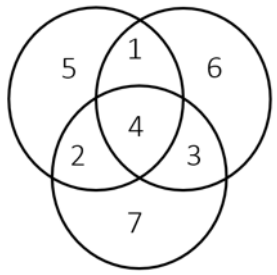


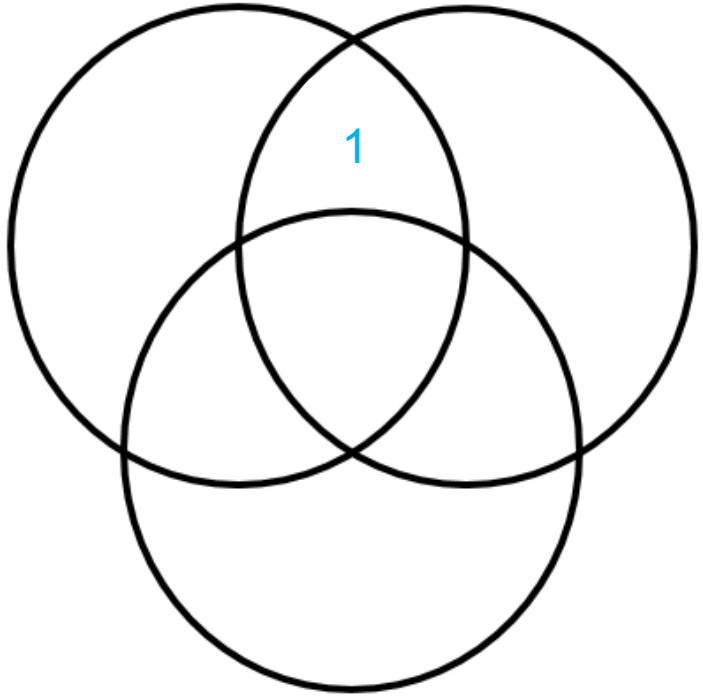
1001 soll übermittelt werden



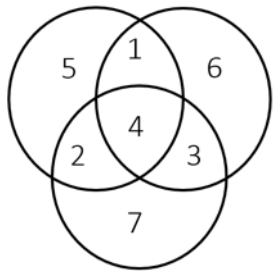


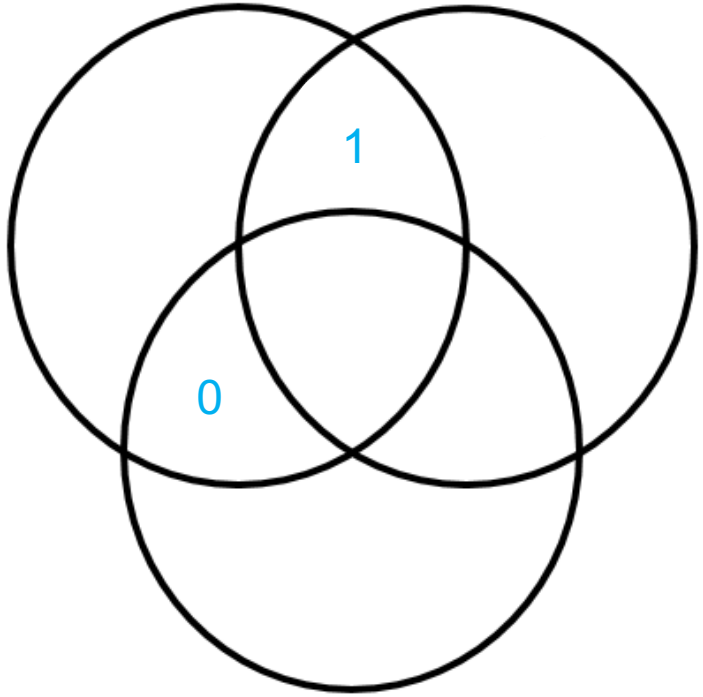
1001 soll übermittelt werden



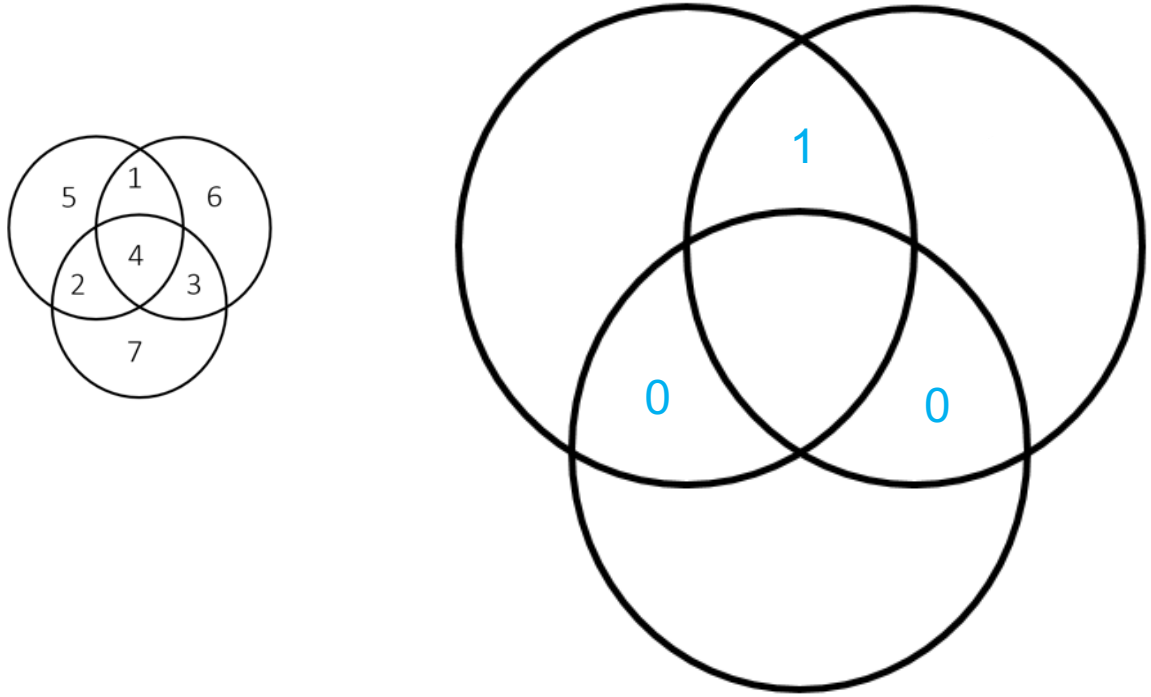


1001 soll übermittelt werden

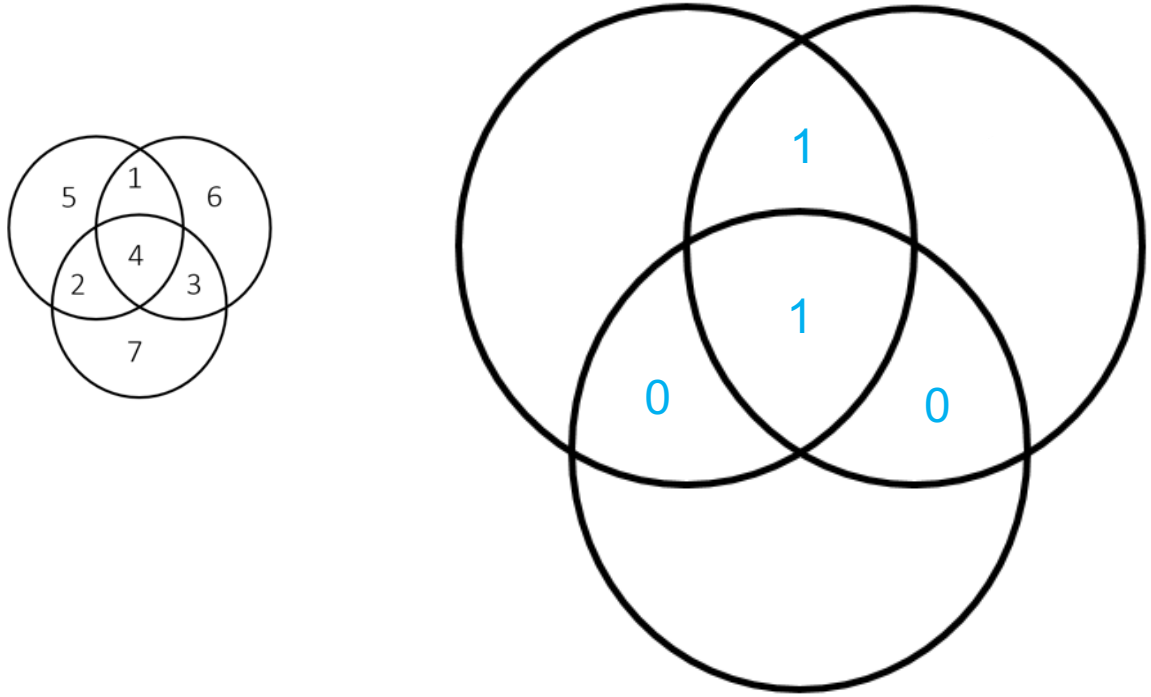




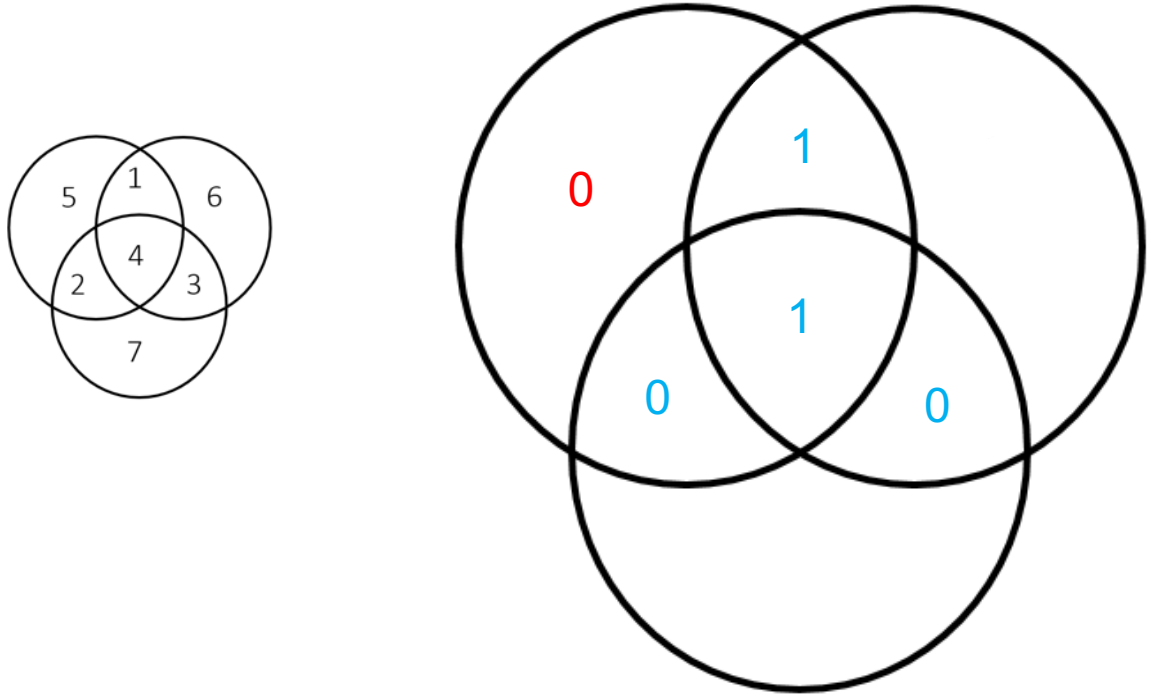
1001 soll übermittelt werden



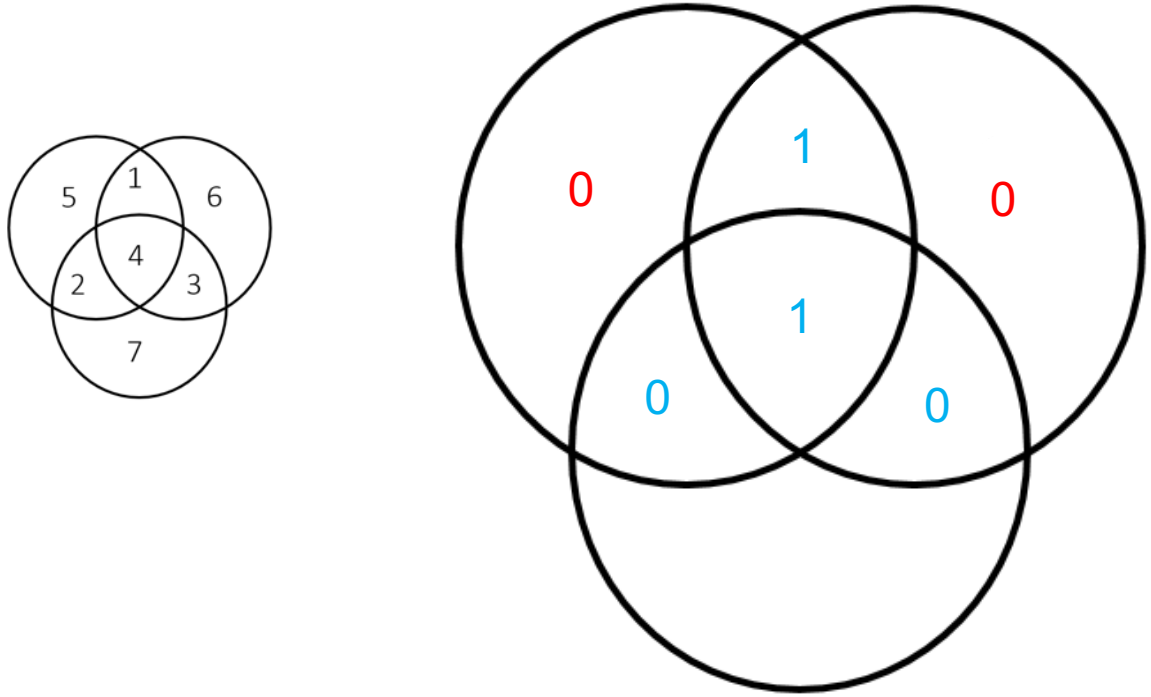
1001 soll übermittelt werden



1001 soll übermittelt werden

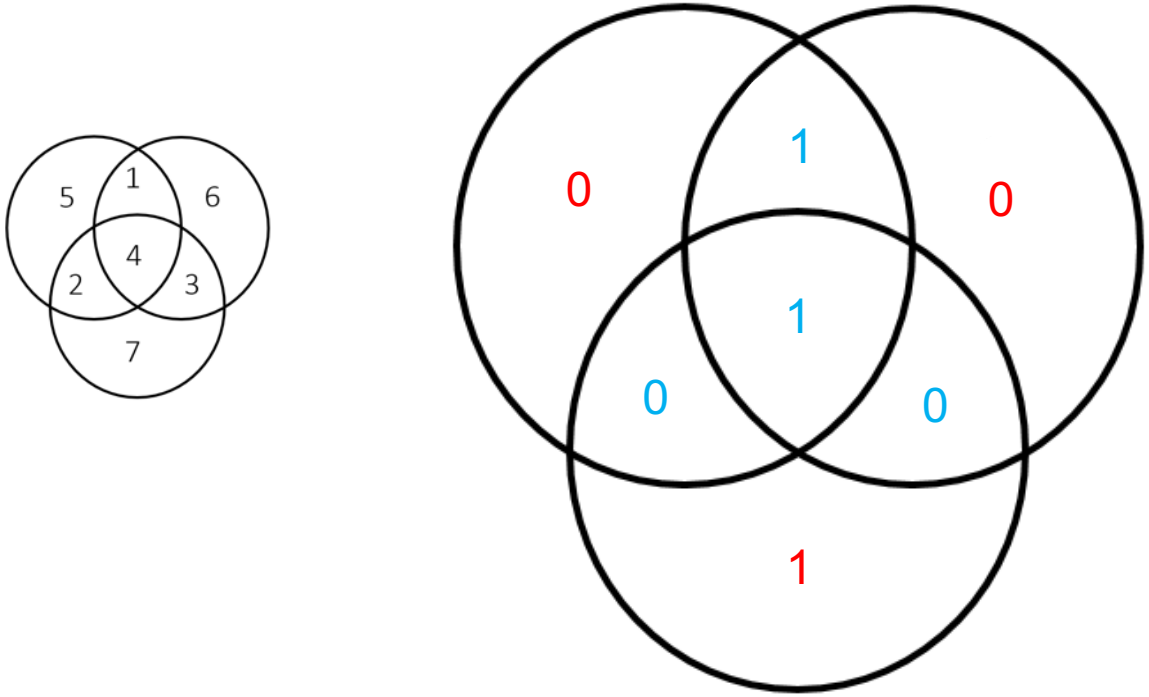


1001 soll übermittelt werden



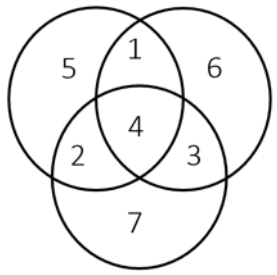
Hamming-Code (konkret: 4 Datenbits – 3 Prüfbits)

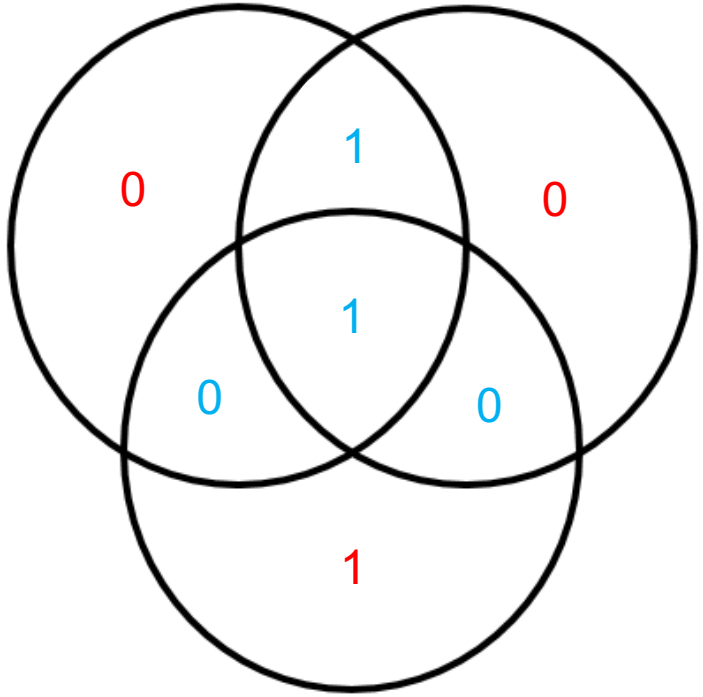
1001 soll übermittelt werden



Hamming-Code (konkret: 4 Datenbits – 3 Prüfbits)

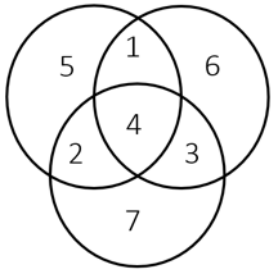
1001 soll übermittelt werden → 1001001 wird übermittelt

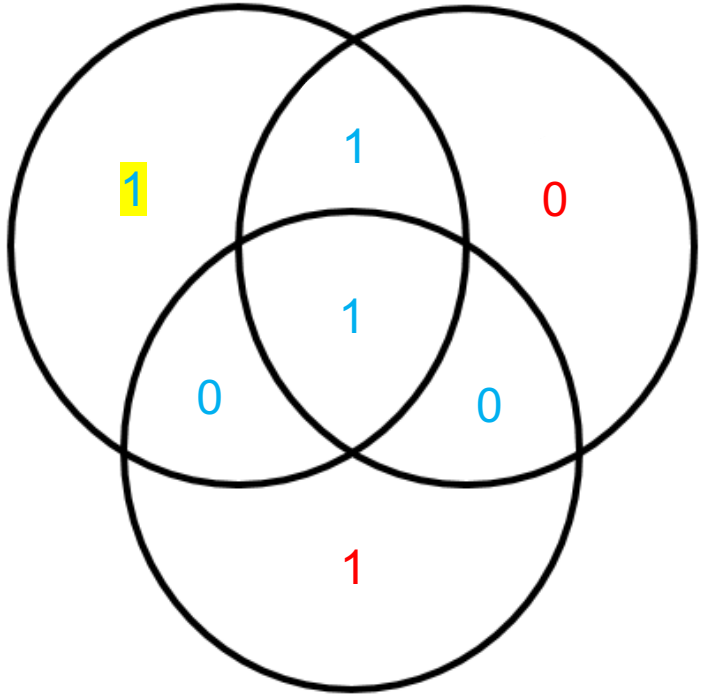




Hamming-Code (konkret: 4 Datenbits – 3 Prüfbits)

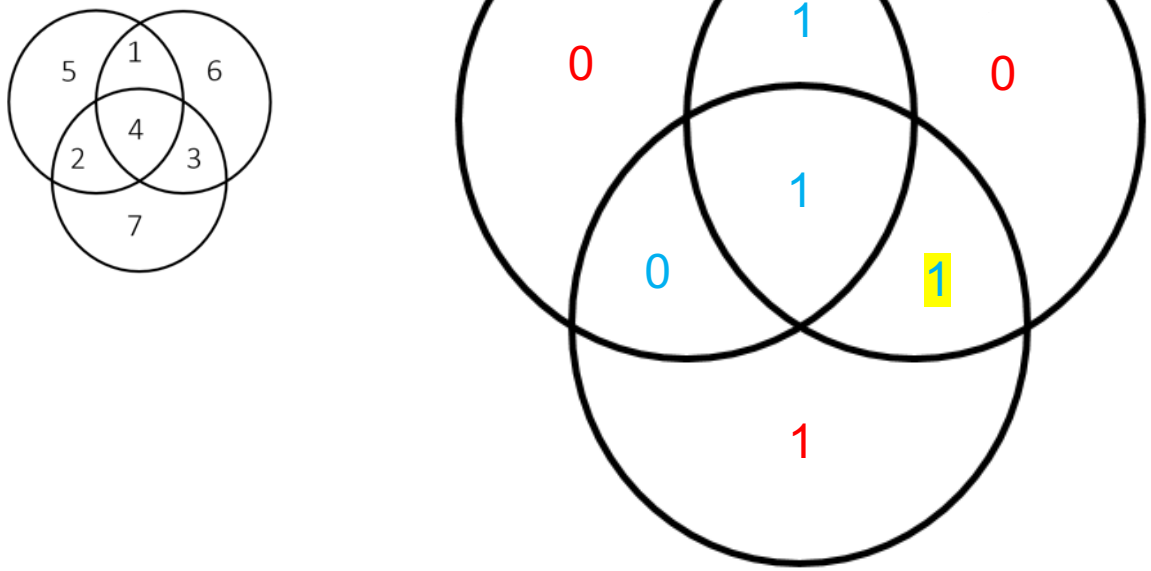
1001 soll übermittelt werden → 1001101 wird übermittelt





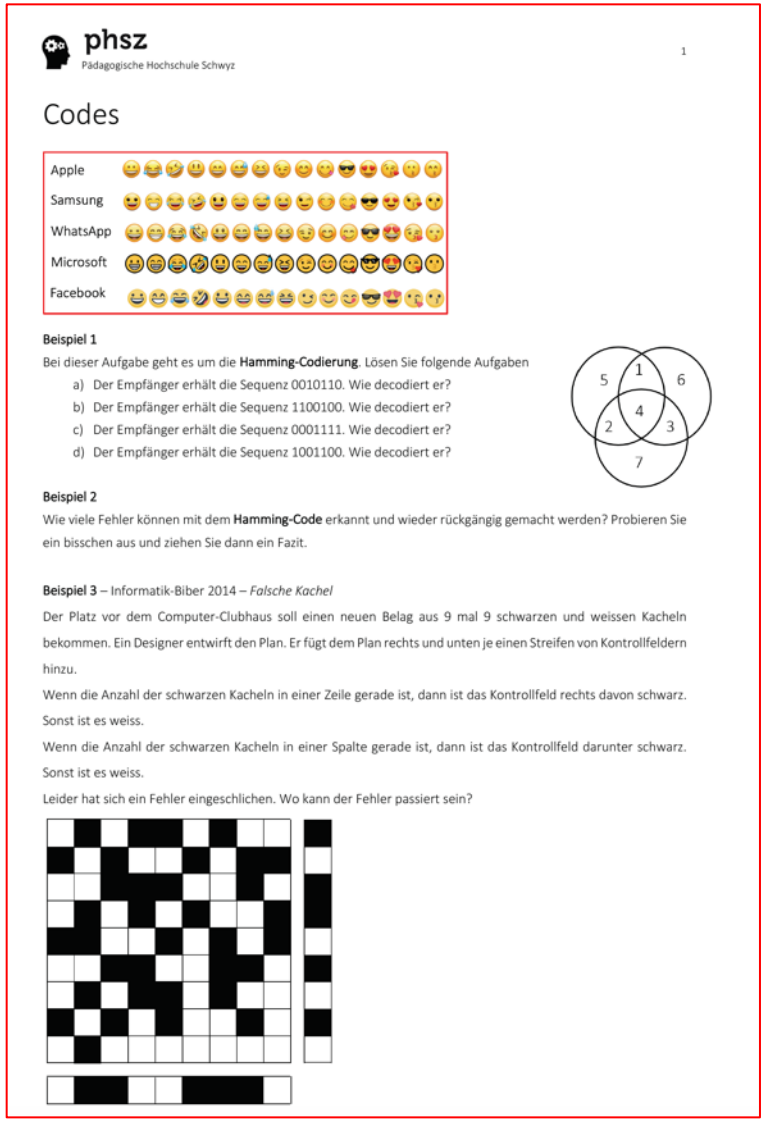
Hamming-Code (konkret: 4 Datenbits – 3 Prüfbits)

1001 soll übermittelt werden → 1011001 wird übermittelt



Aufgaben

Lösen Sie das Beispiel 1 und Beispiel 3.



phsz
Pädagogische Hochschule Schwyz

1

Codes

Apple	
Samsung	
WhatsApp	
Microsoft	
Facebook	

Beispiel 1

Bei dieser Aufgabe geht es um die **Hamming-Codierung**. Lösen Sie folgende Aufgaben

a) Der Empfänger erhält die Sequenz 0010110. Wie decodiert er?
b) Der Empfänger erhält die Sequenz 1100100. Wie decodiert er?
c) Der Empfänger erhält die Sequenz 0001111. Wie decodiert er?
d) Der Empfänger erhält die Sequenz 1001100. Wie decodiert er?

Beispiel 2

Wie viele Fehler können mit dem **Hamming-Code** erkannt und wieder rückgängig gemacht werden? Probieren Sie ein bisschen aus und ziehen Sie dann ein Fazit.

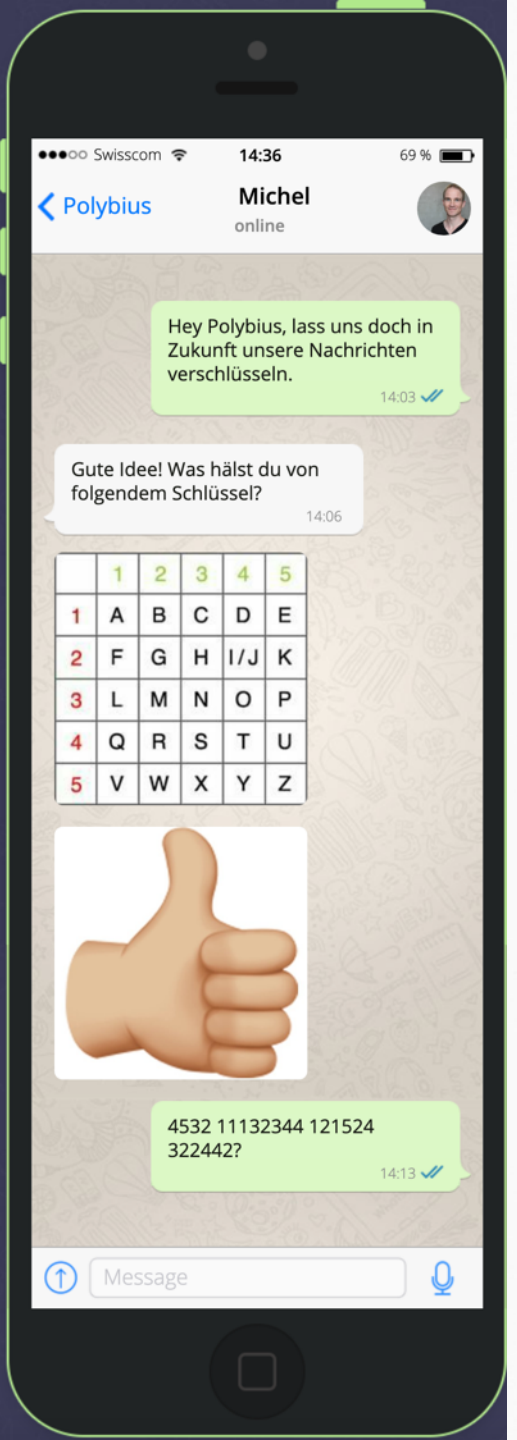
Beispiel 3 – Informatik-Biber 2014 – *Falsche Kachel*

Der Platz vor dem Computer-Clubhaus soll einen neuen Belag aus 9 mal 9 schwarzen und weissen Kacheln bekommen. Ein Designer entwirft den Plan. Er fügt dem Plan rechts und unten je einen Streifen von Kontrollfeldern hinzu.

Wenn die Anzahl der schwarzen Kacheln in einer Zeile gerade ist, dann ist das Kontrollfeld rechts davon schwarz. Sonst ist es weiss.

Wenn die Anzahl der schwarzen Kacheln in einer Spalte gerade ist, dann ist das Kontrollfeld darunter schwarz. Sonst ist es weiss.

Leider hat sich ein Fehler eingeschlichen. Wo kann der Fehler passiert sein?


Swisscom
14:36
69 %
Polybius
Michel
online
Hey Polybius, lass uns doch in Zukunft unsere Nachrichten verschlüsseln.
14:03
Gute Idee! Was hälst du von folgendem Schlüssel?
14:06
1 2 3 4 5
1 A B C D E
2 F G H I/J K
3 L M N O P
4 Q R S T U
5 V W X Y Z
4532 11132344 121524 322442?
14:13
Message

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

4532 11132344 121524 322442?

14:13

Kryptographie = Codierung?

26 Möglichkeiten

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1 Möglichkeiten

25! = 15‘511‘210‘040‘000‘000‘000‘000‘000

26 Möglichkeiten

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1 Möglichkeiten

25! = 15‘511‘210‘040‘000‘000‘~~000‘000‘000~~ Sekunden

1 Milliarde Möglichkeiten pro Sekunde.

26 Möglichkeiten

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1 Möglichkeiten

25! = 15‘511‘210‘~~040‘000‘000~~‘~~000‘000‘000~~ Sekunden

1 Milliarde Computer mit 1 Milliarde Möglichkeiten pro Sekunde.

26 Möglichkeiten

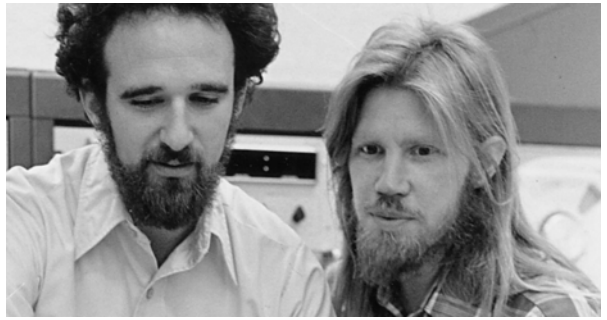
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

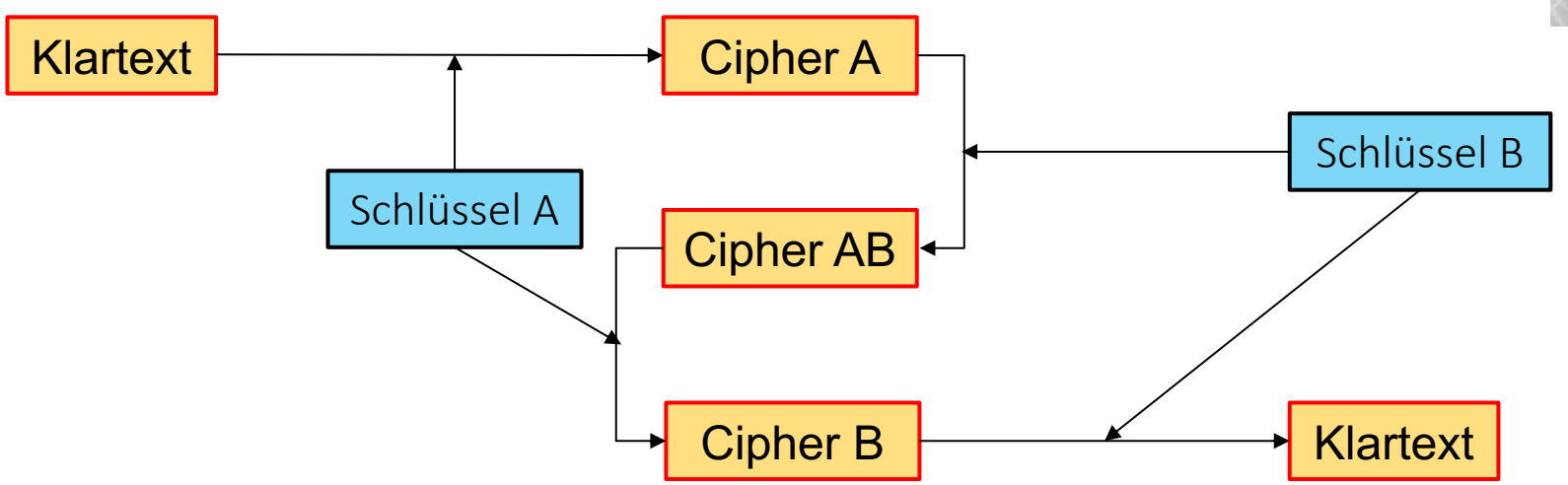
1 Möglichkeiten

25! = 15‘511‘210‘~~040‘000‘000~~‘~~000‘000‘000~~ Sekunden = 179.5 d

1 Milliarde Computer mit 1 Milliarde Möglichkeiten pro Sekunde.

Schlüsselaustausch – Diffie/Hellman





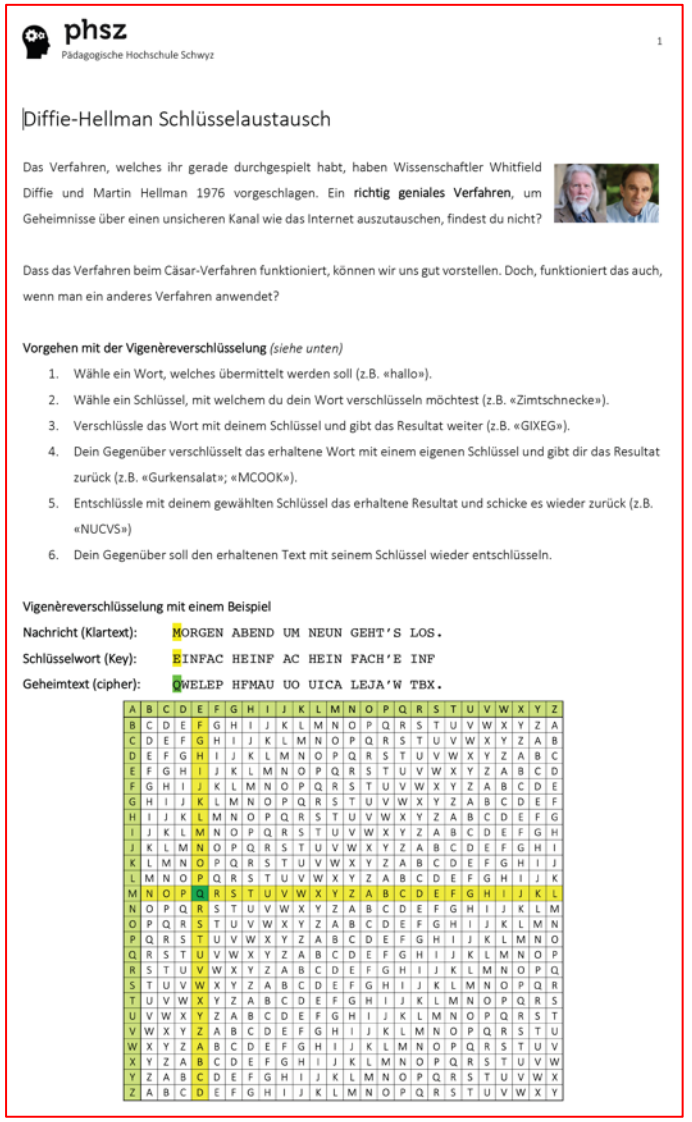
Vorteil Kein Schlüsselaustausch nötig

Schlüsselaustausch – Diffie/Hellman (mit Vigenèreverschlüsselung)

Text: HALLO **Cipher:**

Passwort: EINFACH

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



phsz
Pädagogische Hochschule Schwyz

1

Diffie-Hellman Schlüsselaustausch

Das Verfahren, welches ihr gerade durchgespielt habt, haben Wissenschaftler Whitfield Diffie und Martin Hellman 1976 vorgeschlagen. Ein **richtig geniales Verfahren**, um Geheimnisse über einen unsicheren Kanal wie das Internet auszutauschen, findest du nicht?

Dass das Verfahren beim Cäsar-Verfahren funktioniert, können wir uns gut vorstellen. Doch, funktioniert das auch, wenn man ein anderes Verfahren anwendet?

Vorgehen mit der Vigenèreverschlüsselung *(siehe unten)*

1. Wähle ein Wort, welches übermittelt werden soll (z.B. «hallo»).
2. Wähle ein Schlüssel, mit welchem du dein Wort verschlüsseln möchtest (z.B. «Zimtschnecke»).
3. Verschlüssle das Wort mit deinem Schlüssel und gibt das Resultat weiter (z.B. «GIXEG»).
4. Dein Gegenüber verschlüsselt das erhaltene Wort mit einem eigenen Schlüssel und gibt dir das Resultat zurück (z.B. «Gurkensalat»; «MCOOK»).
5. Entschlüssle mit deinem gewählten Schlüssel das erhaltene Resultat und schicke es wieder zurück (z.B. «NUCVS»)
6. Dein Gegenüber soll den erhaltenen Text mit seinem Schlüssel wieder entschlüsseln.

Vigenèreverschlüsselung mit einem Beispiel

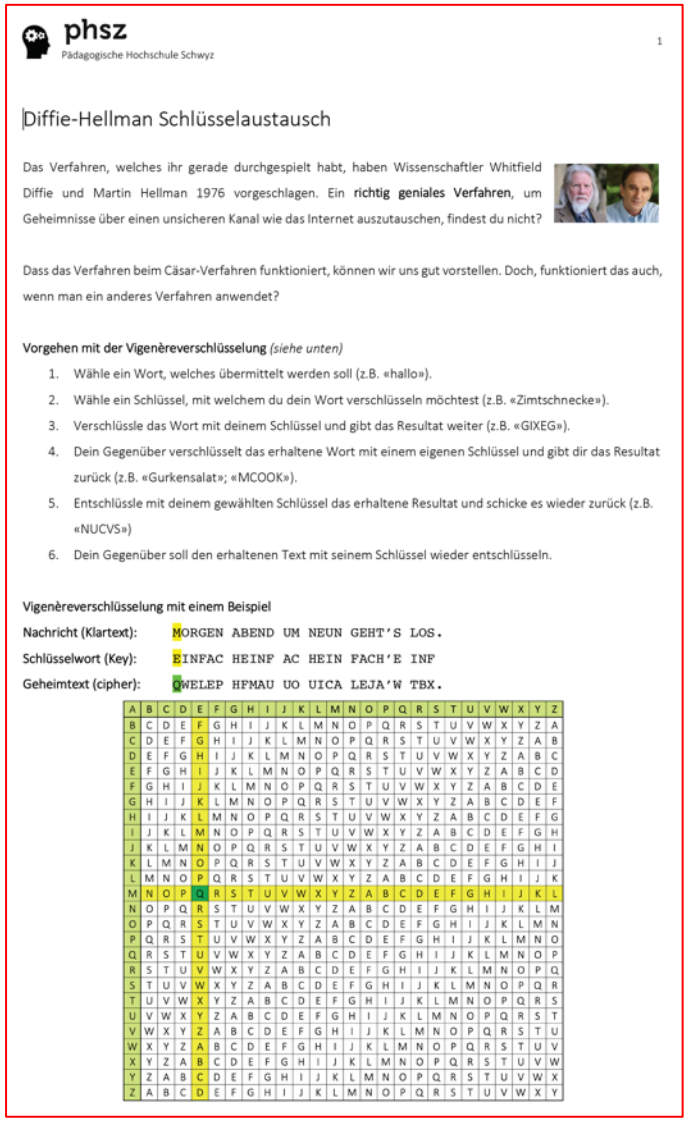
Nachricht (Klartext): MORGEN ABEND UM NEUN GEHT'S LOS.
Schlüsselwort (Key): EINFAC HEINF AC HEIN FACH'E INF
Geheimtext (cipher): QWELEP HFMAU UO UICA LEJA'W TBX.

Schlüsselaustausch – Diffie/Hellman (mit Vigenèreverschlüsselung)

Text: HALLO Cipher:

Passwort: EINFACH

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



phsz
Pädagogische Hochschule Schwyz

1

Diffie-Hellman Schlüsselaustausch

Das Verfahren, welches ihr gerade durchgespielt habt, haben Wissenschaftler Whitfield Diffie und Martin Hellman 1976 vorgeschlagen. Ein **richtig geniales Verfahren**, um Geheimnisse über einen unsicheren Kanal wie das Internet auszutauschen, findest du nicht?

Dass das Verfahren beim Cäsar-Verfahren funktioniert, können wir uns gut vorstellen. Doch, funktioniert das auch, wenn man ein anderes Verfahren anwendet?

Vorgehen mit der Vigenèreverschlüsselung *(siehe unten)*

1. Wähle ein Wort, welches übermittelt werden soll (z.B. «hallo»).
2. Wähle ein Schlüssel, mit welchem du dein Wort verschlüsseln möchtest (z.B. «Zimtschnecke»).
3. Verschlüssle das Wort mit deinem Schlüssel und gibt das Resultat weiter (z.B. «GIXEG»).
4. Dein Gegenüber verschlüsselt das erhaltene Wort mit einem eigenen Schlüssel und gibt dir das Resultat zurück (z.B. «Gurkensalat»; «MCOOK»).
5. Entschlüssle mit deinem gewählten Schlüssel das erhaltene Resultat und schicke es wieder zurück (z.B. «NUCVS»)
6. Dein Gegenüber soll den erhaltenen Text mit seinem Schlüssel wieder entschlüsseln.

Vigenèreverschlüsselung mit einem Beispiel

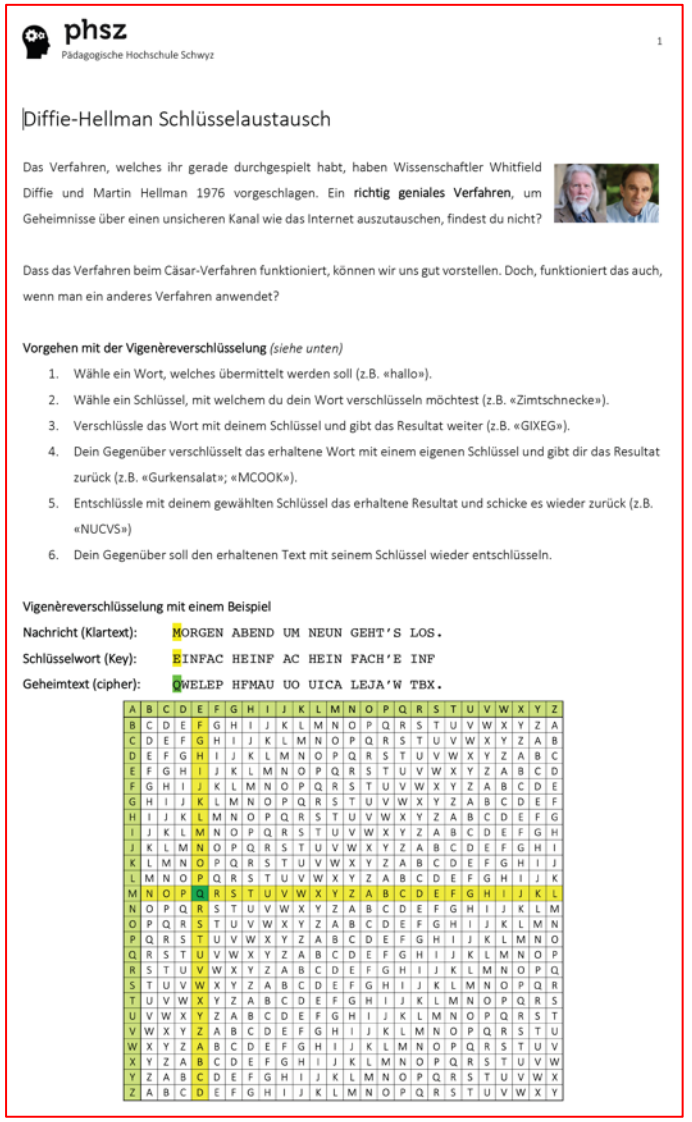
Nachricht (Klartext): MORGEN ABEND UM NEUN GEHT'S LOS.
Schlüsselwort (Key): EINFAC HEINF AC HEIN FACH'E INF
Geheimtext (cipher): QWELEP HFMAU UO UICA LEJA'W TBX.

Schlüsselaustausch – Diffie/Hellman (mit Vigenèreverschlüsselung)

Text: HALLO Cipher: L

Passwort: EINFACH

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



phsz
Pädagogische Hochschule Schwyz

1

Diffie-Hellman Schlüsselaustausch

Das Verfahren, welches ihr gerade durchgespielt habt, haben Wissenschaftler Whitfield Diffie und Martin Hellman 1976 vorgeschlagen. Ein **richtig geniales Verfahren**, um Geheimnisse über einen unsicheren Kanal wie das Internet auszutauschen, findest du nicht?

Dass das Verfahren beim Cäsar-Verfahren funktioniert, können wir uns gut vorstellen. Doch, funktioniert das auch, wenn man ein anderes Verfahren anwendet?

Vorgehen mit der Vigenèreverschlüsselung *(siehe unten)*

1. Wähle ein Wort, welches übermittelt werden soll (z.B. «hallo»).
2. Wähle ein Schlüssel, mit welchem du dein Wort verschlüsseln möchtest (z.B. «Zimtschnecke»).
3. Verschlüssle das Wort mit deinem Schlüssel und gibt das Resultat weiter (z.B. «GIXEG»).
4. Dein Gegenüber verschlüsselt das erhaltene Wort mit einem eigenen Schlüssel und gibt dir das Resultat zurück (z.B. «Gurkensalat»; «MCOOK»).
5. Entschlüssle mit deinem gewählten Schlüssel das erhaltene Resultat und schicke es wieder zurück (z.B. «NUCVS»)
6. Dein Gegenüber soll den erhaltenen Text mit seinem Schlüssel wieder entschlüsseln.

Vigenèreverschlüsselung mit einem Beispiel

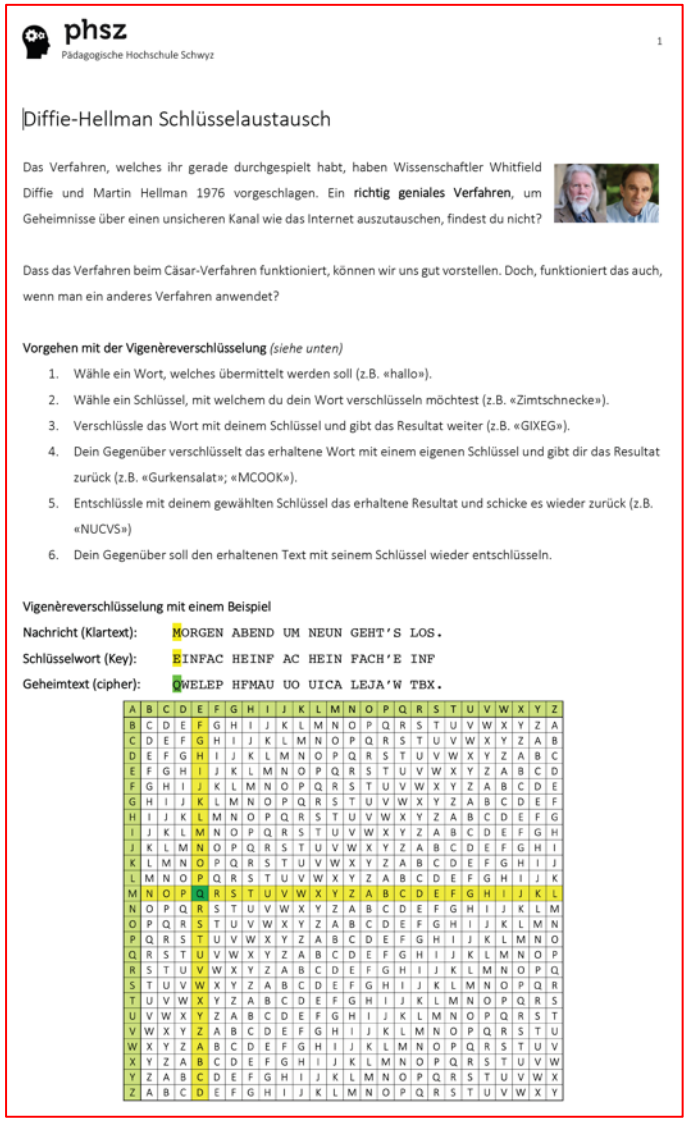
Nachricht (Klartext): MORGEN ABEND UM NEUN GEHT'S LOS.
Schlüsselwort (Key): EINFAC HEINF AC HEIN FACH'E INF
Geheimtext (cipher): QWELEP HFMAU UO UICA LEJA'W TBX.

Schlüsselaustausch – Diffie/Hellman (mit Vigenèreverschlüsselung)

Text: HALLO Cipher: LI

Passwort: EINFACH

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



phsz
Pädagogische Hochschule Schwyz

1

Diffie-Hellman Schlüsselaustausch

Das Verfahren, welches ihr gerade durchgespielt habt, haben Wissenschaftler Whitfield Diffie und Martin Hellman 1976 vorgeschlagen. Ein **richtig geniales Verfahren**, um Geheimnisse über einen unsicheren Kanal wie das Internet auszutauschen, findest du nicht?

Dass das Verfahren beim Cäsar-Verfahren funktioniert, können wir uns gut vorstellen. Doch, funktioniert das auch, wenn man ein anderes Verfahren anwendet?

Vorgehen mit der Vigenèreverschlüsselung *(siehe unten)*

1. Wähle ein Wort, welches übermittelt werden soll (z.B. «hallo»).
2. Wähle ein Schlüssel, mit welchem du dein Wort verschlüsseln möchtest (z.B. «Zimtschnecke»).
3. Verschlüssle das Wort mit deinem Schlüssel und gibt das Resultat weiter (z.B. «GIXEG»).
4. Dein Gegenüber verschlüsselt das erhaltene Wort mit einem eigenen Schlüssel und gibt dir das Resultat zurück (z.B. «Gurkensalat»; «MCOOK»).
5. Entschlüssle mit deinem gewählten Schlüssel das erhaltene Resultat und schicke es wieder zurück (z.B. «NUCVS»)
6. Dein Gegenüber soll den erhaltenen Text mit seinem Schlüssel wieder entschlüsseln.

Vigenèreverschlüsselung mit einem Beispiel

Nachricht (Klartext): MORGEN ABEND UM NEUN GEHT'S LOS.
Schlüsselwort (Key): EINFAC HEINF AC HEIN FACH'E INF
Geheimtext (cipher): QWELEP HFMAU UO UICA LEJA'W TBX.

Es bleibt wohl immer relevant, Informationen möglichst effizient codieren zu können!

Beschränkter Platz	Beschränkte Zeit	Beschränkte Anzahl Fehler