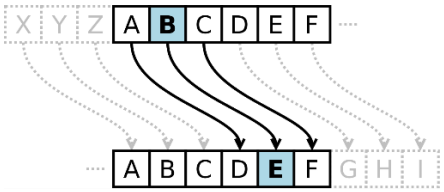
CAESAR VERSCHLÜSSELUNG

Die Caesar-Verschlüsselung ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert. Als eines der einfachsten und unsichersten Verfahren dient es heute hauptsächlich dazu, Grundprinzipien der Kryptologie anschaulich darzustellen. Der Einfachheit halber werden oftmals nur die 26 Buchstaben des lateinischen Alphabets ohne Unterscheidung von Groß- und Kleinbuchstaben als Alphabet für Klartext und Geheimtext verwendet und Sonderzeichen, Satzzeichen usw. nicht beachtet.

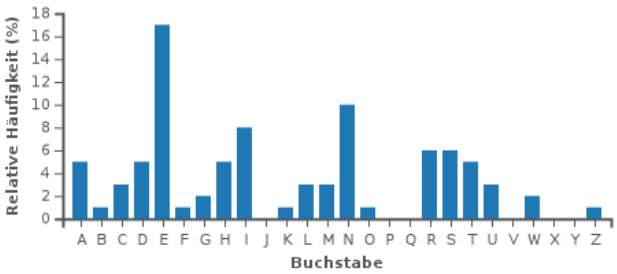
Bei der Verschlüsselung wird jeder Buchstabe des Klartexts auf einen Geheimtextbuchstaben abgebildet. Diese Abbildung ergibt sich, indem man die Zeichen eines geordneten Alphabets um eine bestimmte Anzahl zyklisch nach rechts verschiebt (rotiert); zyklisch bedeutet, dass man beim Verschieben über Z hinaus wieder bei A anfangend weiterzählt. Die Anzahl der verschobenen Zeichen bildet den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt. Beispiel für eine Verschiebung um drei Zeichen:



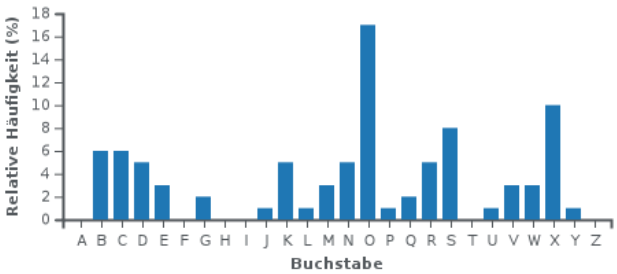
Aus dem Klartext „caesar“ wird somit der Geheimtext „FDHVDU“. Für die Entschlüsselung wird das Alphabet um dieselbe Anzahl Zeichen nach links rotiert.

Wie alle monoalphabetischen Verschlüsselungsverfahren bietet auch die Verschiebechiffre keine hinreichende Sicherheit gegen unbefugte Entzifferung und kann sehr leicht „geknackt“ werden. Die in der natürlichen Sprache ungleiche Verteilung der Buchstaben wird durch diese Art der Verschlüsselung nicht verborgen, so dass eine Häufigkeitsanalyse das Wirken einer einfachen monoalphabetischen Substitution enthüllt.

Das folgende Diagramm zeigt die Häufigkeitsverteilung der Buchstaben in einem längeren Text in deutscher Sprache:

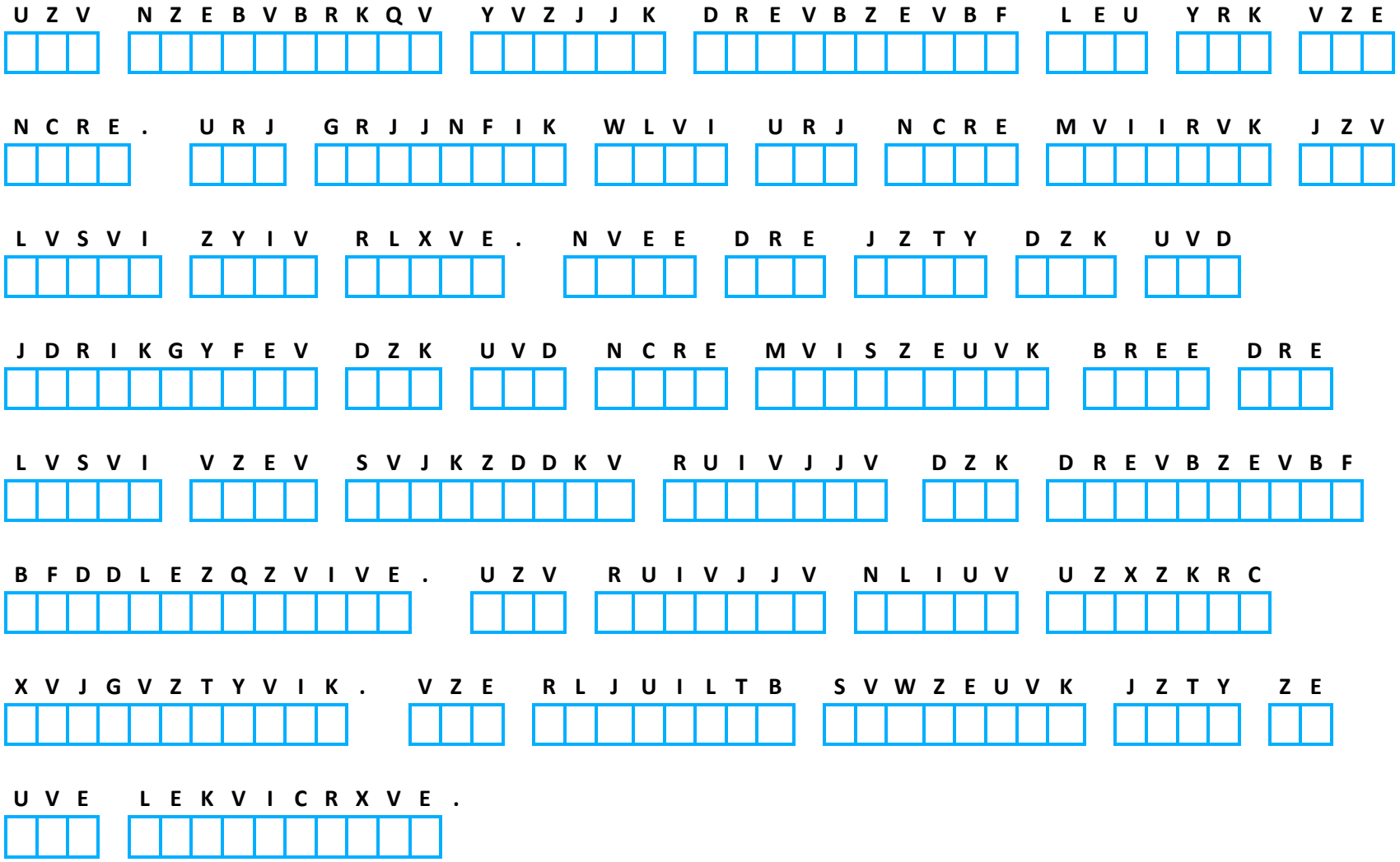


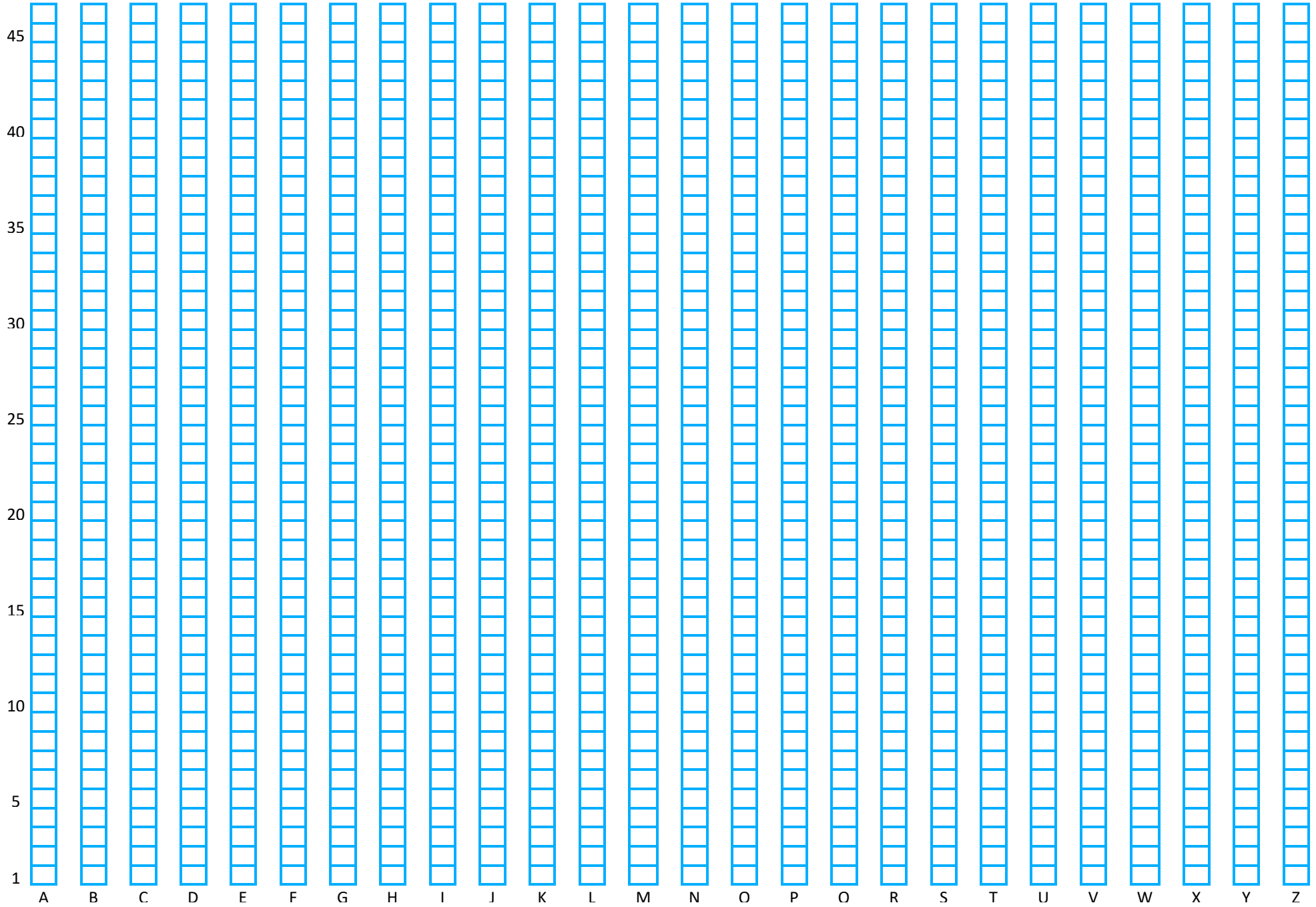
Wie zu erwarten, ist der häufigste Buchstabe E, gefolgt von N und I, wie es im Deutschen üblicherweise der Fall ist. Wird der Text mit dem Schlüssel 10 (oder anders gesagt, mit dem Schlüsselbuchstaben J) chiffriert, erhält man einen Geheimtext, der folgende Häufigkeitsverteilung besitzt:

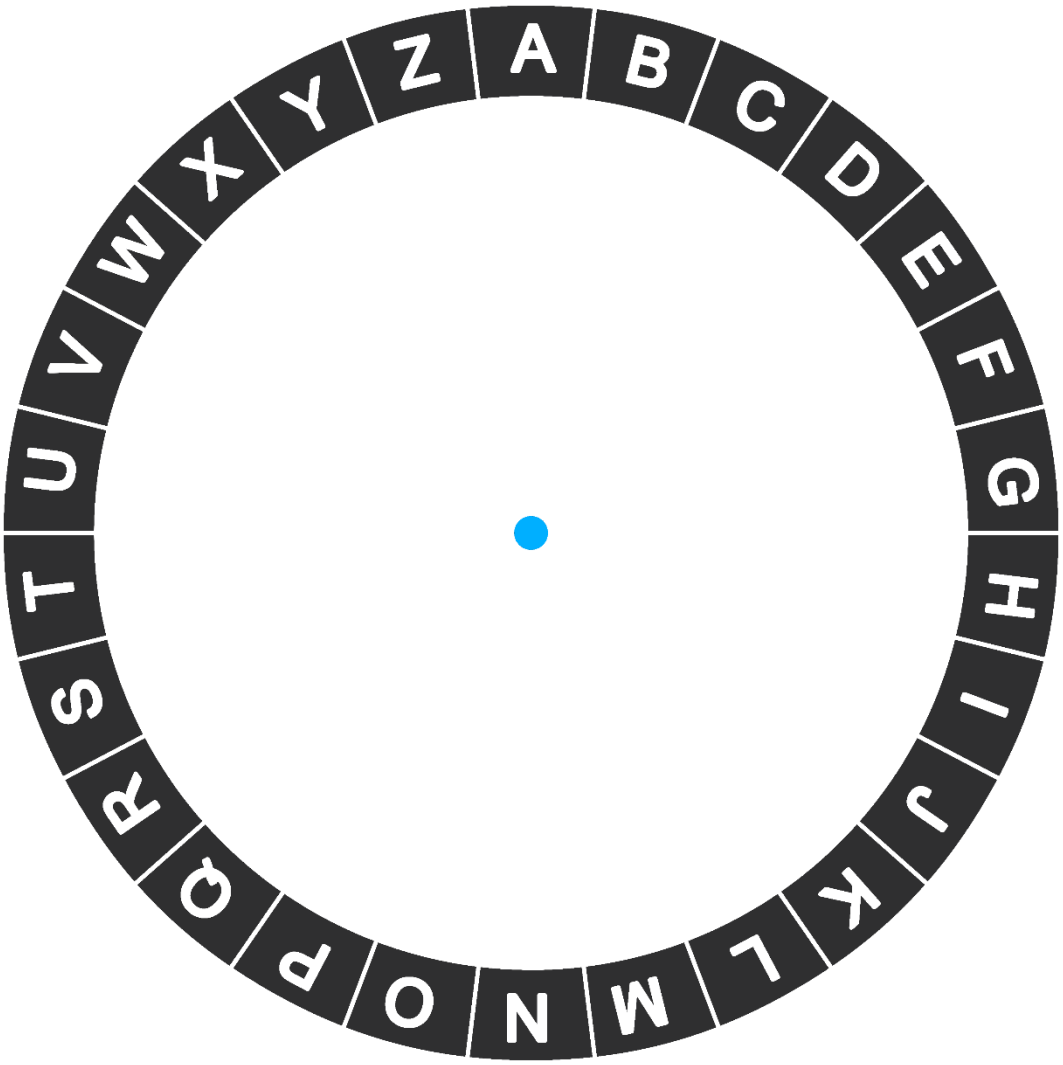


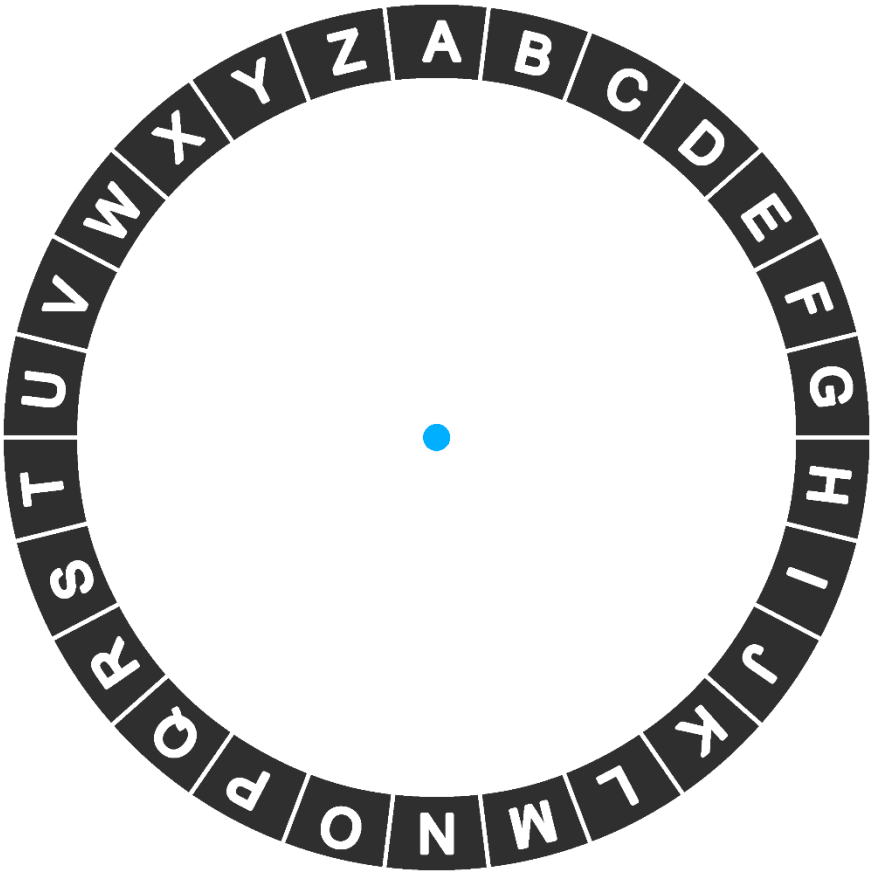
Der häufigste Buchstabe ist hier O, gefolgt von X und S. Man erkennt auf den ersten Blick die Verschiebung des deutschen „Häufigkeitsgebirges“ um zehn Stellen nach hinten und besitzt damit den Schlüssel. Voraussetzung ist lediglich, dass man die Verteilung der Zeichen des Urtextes vorhersagen kann.

Quelle: https://de.wikipedia.org/wiki/Caesar-Verschl%C3%BCsselung


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


45
40
35
30
25
20
15
10
5
1
A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
O
R
S
T
U
V
W
X
Y
Z


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

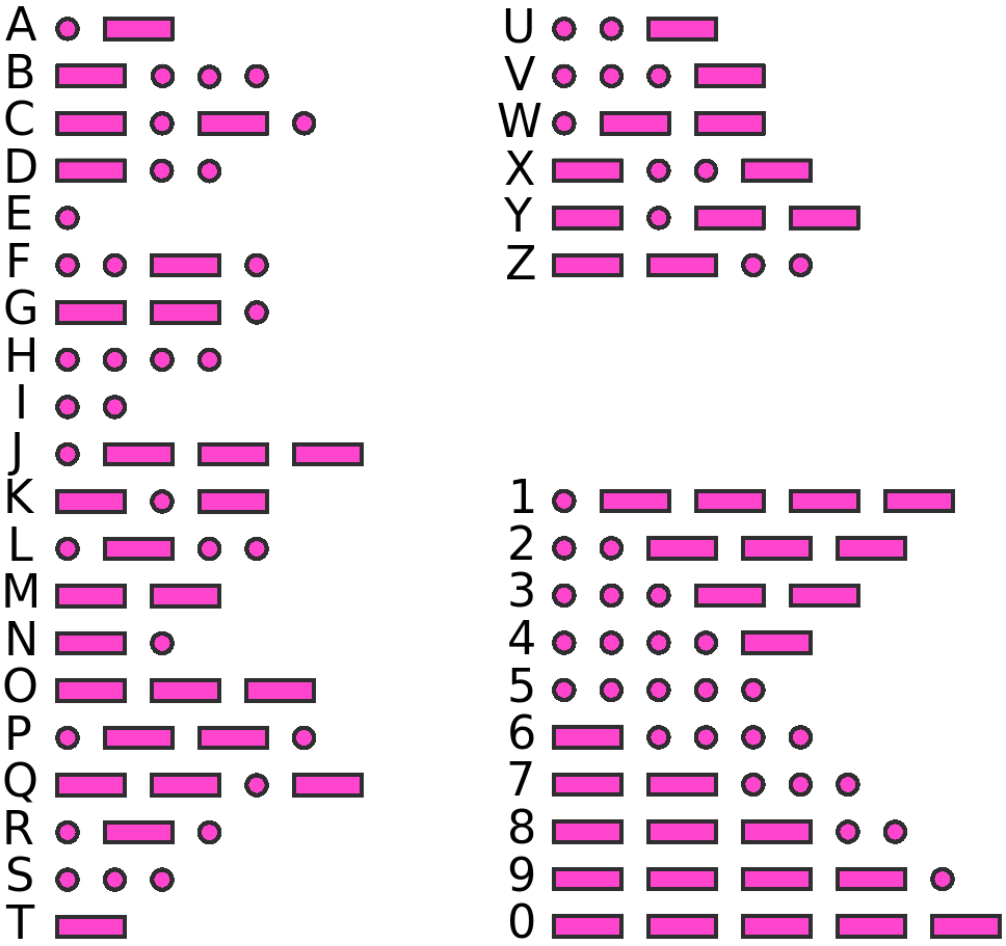

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

MORSE ALPHABET

Das Morsealphabet , manchmal auch Morsezeichen oder Morsecode genannt, ist ein Zeichensatz zur Übermittlung von Buchstaben, Ziffern und übrigen Zeichen. Dabei wird ein direktes Signal ein- und ausgeschaltet. Es besteht aus drei Symbolen: kurzes Signal, langes Signal und Pause.

Der Code kann als Tonsignal, als Funksignal, als elektrischer Puls mit einer Morsetaste über eine Telefonleitung, mechanisch oder optisch (etwa mit blinkendem Licht) übertragen werden – oder auch mit jedem sonstigen Medium, mit dem zwei verschiedene Zustände (wie etwa Ton oder kein Ton) eindeutig und in der zeitlichen Länge variierbar dargestellt werden können. Dieses Übertragungsverfahren nennt man Morsetelegrafie.

Das manchmal bei Notfällen beschriebene Morsen durch Klopfen an metallischen Verbindungen erfüllt diese Forderung daher nur bedingt, ist aber mit einiger Übung aufgrund des charakteristischen Rhythmus von Morsezeichen verständlich. Diese Hörtechnik ist abgeleitet von den „Klopfern“ aus der Anfangszeit der Telegrafentechnik, bestehend aus einem kräftigen Relais in einem akustischen Hohlspiegel, der den Klang der Morsezeichen schon vor der Erfindung des Lautsprechers selbst in größeren Betriebsräumen hörbar machte.



Quelle: https://de.wikipedia.org/wiki/Morsezeichen

Das Dualsystem (lat. dualis „zwei enthaltend“), auch Zweiersystem oder Binärsystem genannt, ist ein Zahlensystem, das zur Darstellung von Zahlen nur zwei verschiedene Ziffern benutzt.

Im üblichen Dezimalsystem werden die Ziffern 0 bis 9 verwendet. Im Dualsystem hingegen werden Zahlen nur mit den Ziffern des Wertes null und eins dargestellt. Oft werden für diese Ziffern die Symbole 0 und 1 verwendet.

Aufgrund seiner Bedeutung in der Digitaltechnik ist es neben dem Dezimalsystem das wichtigste Zahlensystem.

Die Zahldarstellungen im Dualsystem werden auch Dualzahlen oder Binärzahlen genannt. Letztere ist die allgemeinere Bezeichnung, da diese auch einfach für binärcodierte Zahlen stehen kann. Der Begriff Binärzahl spezifiziert die Darstellungsweise einer Zahl also nicht näher, er sagt nur aus, dass zwei verschiedene Ziffern verwendet werden.

Um eine Dualzahl in die entsprechende Dezimalzahl umzurechnen, werden alle Ziffern jeweils mit ihrem Stellenwert (entsprechende Zweierpotenz) multipliziert und dann addiert.

Beispiel:

$$1010_{(2)} = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1 \cdot 2^3 + 1 \cdot 2^1 = 8 + 2 = 10_{(10)}$$

Dieses Verfahren kann auch in Form einer Tabelle aufgeschrieben werden. Dazu notiert man die einzelnen Ziffern einer Dualzahl in Spalten, die mit dem jeweiligen Stellenwert der Ziffer überschrieben sind. In der folgenden Tabelle ist der Stellenwert orange hinterlegt. In jeder der drei Zeilen des weißen Teils steht eine Dualzahl:

	Stellenwert							
	32	16	8	4	2	1		
Dualzahl	0	0	0	1	0	1	5	Dezimalzahl
	1	0	0	0	1	1	35	
	0	0	1	0	1	0	10	

Man addiert nun alle Stellenwerte, die über den Einsen der Dualzahl stehen und erhält die entsprechende grün hinterlegte Dezimalzahl. Um zum Beispiel den Dezimalwert der dritten Dualzahl zu errechnen, werden die Stellenwerte 8 und 2 addiert. Das Ergebnis ist 10.

Diese Tabellenmethode ist auch für Stellenwertsysteme zu anderen Basen möglich; die Besonderheit im Dualsystem ist, dass der jeweilige Feldeintrag ('0' oder '1') nicht erst mit der Wertigkeit der Stelle multipliziert werden muss, sondern direkt als Auswahl-Flag ('nein' / 'ja') dieser Stellenwertigkeit zur Addition verwendet werden kann.

Quelle: https://de.wikipedia.org/wiki/Dualsystem

ASCII

7-BIT-ZEICHENKODIERUNG

Der American Standard Code for Information Interchange (ASCII) ist eine 7-Bit-Zeichenkodierung.

Die druckbaren Zeichen umfassen das lateinische Alphabet in Groß- und Kleinschreibung, die zehn arabischen Ziffern sowie einige Interpunktionszeichen und andere Sonderzeichen. Der Zeichenvorrat entspricht weitgehend dem einer Tastatur oder Schreibmaschine für die englische Sprache. In Computern und anderen elektronischen Geräten, die Text darstellen, wird dieser in der Regel gemäß ASCII oder abwärtskompatibel (ISO 8859, Unicode) dazu gespeichert.

Jedem Zeichen wird ein Bitmuster aus 7 Bit zugeordnet. Da jedes Bit zwei Werte annehmen kann, gibt es 27 = 128 verschiedene Bitmuster, die auch als die ganzen Zahlen 0–127 interpretiert werden können.

Das für ASCII nicht benutzte achte Bit kann für Fehlerkorrekturzwecke (Paritätsbit) auf den Kommunikationsleitungen oder für andere Steuerungsaufgaben verwendet werden. Heute wird es aber fast immer zur Erweiterung von ASCII auf einen 8-Bit-Code verwendet. Diese Erweiterungen sind mit dem ursprünglichen ASCII weitgehend kompatibel, so dass alle im ASCII definierten Zeichen auch in den verschiedenen Erweiterungen durch die gleichen Bitmuster kodiert werden. Die einfachsten Erweiterungen sind Kodierungen mit sprachspezifischen Zeichen (Ä, ä, Ö, ö, Ü, ü, ß, etc.), die nicht im lateinischen Grundalphabet enthalten sind.

Dez	ASCII
0	NUL
1	SOH
2	STX
3	ETX
4	EOT
5	ENQ
6	ACK
7	BEL
8	BS
9	HT
10	LF
11	VT
12	FF
13	CR
14	SO
15	SI
16	DLE
17	DC1
18	DC2
19	DC3
20	DC4
21	NAK
22	SYN
23	ETB
24	CAN
25	EM
26	SUB
27	ESC
28	FS
29	GS
30	RS
31	US

Dez	ASCII
32	SP
33	!
34	"
35	#
36	$
37	%
38	&
39	'
40	(
41	)
42	*
43	+
44	,
45	-
46	.
47	/
48	0
49	1
50	2
51	3
52	4
53	5
54	6
55	7
56	8
57	9
58	:
59	;
60	<
61	=
62	>
63	?

Dez	ASCII
64	@
65	A
66	B
67	C
68	D
69	E
70	F
71	G
72	H
73	I
74	J
75	K
76	L
77	M
78	N
79	O
80	P
81	Q
82	R
83	S
84	T
85	U
86	V
87	W
88	X
89	Y
90	Z
91	[
92	\
93	]
94	^
95	_

Dez	ASCII
96	`
97	a
98	b
99	c
100	d
101	e
102	f
103	g
104	h
105	i
106	j
107	k
108	l
109	m
110	n
111	o
112	p
113	q
114	r
115	s
116	t
117	u
118	v
119	w
120	x
121	y
122	z
123	{
124	|
125	}
126	~
127	DEL

Quelle: https://de.wikipedia.org/wiki/American_Standard_Code_for_Information_Interchange


0 1 1 0 1 0 0 0
0 1 1 1 0 1 0 0
0 1 1 1 0 1 0 0
0 1 1 1 0 0 0 0
0 0 1 1 1 0 1 0
0 0 1 0 1 1 1 1
0 0 1 0 1 1 1 1
0 0 1 1 0 0 0 1
0 0 1 1 1 0 0 1
0 0 1 1 0 0 1 0
0 0 1 0 1 1 1 0
0 0 1 1 0 0 0 1
0 0 1 1 0 1 1 0
0 0 1 1 1 0 0 0
0 0 1 0 1 1 1 0
0 0 1 1 0 1 0 0
0 0 1 0 1 1 1 0
0 0 1 1 0 0 0 1
0 0 1 1 0 1 1 1
0 0 1 1 0 0 1 1