ACSII-Code

Buchstaben und andere Zeichen müssen vom Computer codiert werden, da dieser mit Nullen und Einsen arbeitet. Dafür gibt es einen festgelegten Code, den sogenannten ASCII-Code. ASCII steht für American Standard Code for Information Interchange.

Einen Auszug aus der Codierungstabelle siehst du hier:

Dezimal	Binär		Dezimal	Binär		Dezimal	Binär	
32	00100000	SP	64	01000000	@	96	01100000	`
33	00100001	!	65	01000001	A	97	01100001	a
34	00100010	"	66	01000010	B	98	01100010	b
35	00100011	#	67	01000011	C	99	01100011	c
36	00100100	$	68	01000100	D	100	01100100	d
37	00100101	%	69	01000101	E	101	01100101	e
38	00100110	&	70	01000110	F	102	01100110	f
39	00100111	'	71	01000111	G	103	01100111	g
40	00101000	(	72	01001000	H	104	01101000	h
41	00101001	)	73	01001001	I	105	01101001	i
42	00101010	*	74	01001010	J	106	01101010	j
43	00101011	+	75	01001011	K	107	01101011	k
44	00101100	,	76	01001100	L	108	01101100	l
45	00101101	-	77	01001101	M	109	01101101	m
46	00101110	.	78	01001110	N	110	01101110	n
47	00101111	/	79	01001111	O	111	01101111	o
48	00110000	0	80	01010000	P	112	01110000	p
49	00110001	1	81	01010001	Q	113	01110001	q
50	00110010	2	82	01010010	R	114	01110010	r
51	00110011	3	83	01010011	S	115	01110011	s
52	00110100	4	84	01010100	T	116	01110100	t
53	00110101	5	85	01010101	U	117	01110101	u
54	00110110	6	86	01010110	V	118	01110110	v
55	00110111	7	87	01010111	W	119	01110111	w
56	00111000	8	88	01011000	X	120	01111000	x
57	00111001	9	89	01011001	Y	121	01111001	y
58	00111010	:	90	01011010	Z	122	01111010	z
59	00111011	;	91	01011011	[	123	01111011	{
60	00111100	<	92	01011100	\	124	01111100	|
61	00111101	=	93	01011101	]	125	01111101	}
62	00111110	>	94	01011110	^	126	01111110	~
63	00111111	?	95	01011111	_	127	01111111	DEL

Wir müssen zwischen Codierung und Verschlüsselung unterscheiden. Beim Codieren werden Zeichen in eine Form umgewandelt, mit der Personen oder Computer besser arbeiten können. Die Methode ist dabei für alle öffentlich verfügbar. Beim Verschlüsseln hingegen ist die Geheimhaltung wichtig.

2. Infoblatt: # Verschlüsseln

Verschlüsseln mit dem Computer

Wir wollen verstehen, wie der Computer verschlüsselt. Mathematisch geht es dabei hauptsächlich um das Potenzieren und das Teilen mit Rest. Da der Computer mit sehr großen (Prim-) Zahlen arbeitet und das schwierig nachzuvollziehen ist, betrachten wir ein stark vereinfachtes Beispiel der RSA-Verschlüsselung.

Für die Verschlüsselung werden **zwei Primzahlen** benötigt, deren Produkt festlegt, wie viele unterschiedliche Zeichen es geben kann. Wir wählen **5** und **7**, da wir so jedem Buchstaben und ein paar weiteren Zeichen Zahlen von 2 bis 34 Zeichen zuordnen können, denn 5 mal 7 ist **35**. Wir haben zum Beispiel folgende **Codierung**:

Zahl	2	3	4	**5**	6	7	8	9	**10**	11	12	13	14	15	16	17
Zeichen	A	B	C	**D**	E	F	G	H	**I**	J	K	L	M	N	O	P

18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
Q	R	S	T	U	V	W	X	Y	Z	.	,	?	!	-	(	)

Zusätzlich wird noch **eine Primzahl zum Verschlüsseln** und **eine zum Endschlüsseln** benötigt. Hier verwenden wir sowohl für Verschlüsselung als auch für die Entschlüsselung jeweils die **5**. Die Zahlen sind so gewählt, dass jedem Zeichen genau ein anderes Zeichen zugeordnet wird.

Vorgehensweise Verschlüsselung: Welches Zeichen wollen wir verschlüsseln und mit welcher Zahl ist dieses Zeichen codiert? Diese Zahl wird so oft mit sich selbst multipliziert, wie die Primzahl zur Verschlüsselung lautet. Das Ergebnis teilen wir durch das Produkt unserer beiden Primzahlen und verwenden den Rest. Unser Zeichen wird mit dem Zeichen verschlüsselt, das der Zahl des Restes zugeordnet ist.

Beispiel: Wir wollen das **I** verschlüsseln, es hat die Zahl **10**. Die Primzahl zur Verschlüsselung ist **5**, also rechnen wir: $10^5 = 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 100000$. Unsere Primzahlen sind **5 · 7 (5 · 7 = 35)**. Also rechnen wir 100000 : **35** = 2857 Rest **5**. Die **5** war davor dem **D** zugeordnet. Das heißt, das **I** wird zu einem **D**.

Vorgehensweise Entschlüsselung (= Vorgehensweise Verschlüsselung):
Welches Zeichen wollen wir entschlüsseln und mit welcher Zahl ist dieses Zeichen codiert? Diese Zahl wird so oft mit sich selbst multipliziert, wie die Primzahl zur Entschlüsselung lautet. Das Ergebnis teilen wir durch das Produkt unserer beiden Primzahlen und verwenden den Rest. Unser Zeichen wird mit dem Zeichen verschlüsselt, das der Zahl des Restes zugeordnet ist.

Beispiel: Wir wollen das **D** entschlüsseln, es hat die Zahl **5**. Die Primzahl zur Entschlüsselung ist **5**, also rechnen wir: $5^5 = 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 3125$. Unsere Primzahlen sind **5 · 7 (5 · 7 = 35)**. Also rechnen wir 3125 : **35** = 89 Rest **10**. Die **10** war davor dem **I** zugeordnet. Das heißt, das **D** wird zu einem **I**.

Beim Computer werden sehr große Primzahlen verwendet und alle Primzahlen sind verschieden. Damit ist es schwer die Verschlüsselung zu knacken. Zudem werden statt Dezimalzahlen die Binärzahlen wie beim ACSII-Code verwendet.

Maskieren

Damit die Verschlüsselung nicht wie beim Geheimtext mit Häufigkeitsanalysen geknackt werden können, werden die Zahlen vor dem Verschlüsseln maskiert. Das funktioniert, indem **aus jeweils zwei Zahlen** („Zahl 1“ und „Zahl 2“) **eine neue Zahl berechnet** wird. Dafür wird **eine weitere Zahl** („Große Zahl“) benötigt, die größer ist als die Zahlen, die maskiert werden. Zum Beispiel 36.

Allgemeine Rechnung: Zahl 1 + Zahl 2 · Große Zahl. (Die zweite Zahl wird mit 36 multipliziert und die erste Zahl wird zum Produkt hinzuaddiert.)

Zahl	**2**	3	4	5	6	7	8	9	10	**11**	12	13	14	15	16	17
Zeichen	**A**	B	C	D	E	F	G	H	I	**J**	K	L	M	N	O	P

Vorgehensweise Maskieren: Welches Wort wollen wir maskieren und wie lautet die große Zahl? Welchen Zahlen ist der erste und zweite Buchstabe des Wortes zugeordnet? Wie lauten unsere Rechnung und unsere Maskierungszahl?

Beispiel: Wir wollen das Wort **JA** maskieren und wählen als große Zahl **36**. **J** ist der **11** zugeordnet und **A** der **2**. Wir rechnen: **11** + **2** · 36 = 83. Also ist 83 die Maskierungszahl.

Demaskieren: Wir teilen die Maskierungszahl durch **36** und bestimmen so den Rest: 83 : **36** = **2** Rest **11**. Damit wissen wir die erste Zahl und bekommen auch direkt die zweite Zahl.

Das Wort JAHR sieht nach dem Codieren und Maskieren so aus: 83 693