

# Wechsel in der Start-Sequenz

(Ernst Erich Schnoor)

Zur Darstellung der Sensibilität der im Artikel "[Kryptographische Basisfunktion in Byte-Technik](#)" beschriebenen Funktion wird die **Start Sequenz** im letzten Zeichen um ein **Bit** von „1“ auf „0“ geändert.

Start Sequenz (alt): **Bruno der Braunbär aus Bregenz im Breisgau**

Start Sequenz (neu): **Bruno der Braunbär aus Bregenz im Breisgat**

$$u = 75 = 1110101$$

$$t = 74 = 1110100$$

42 72 75 6E 6F 20 64 65 72 20 42 72 61 75 6E 62 84 72 20 61 75  
73 20 42 72 65 67 65 6E 7A 20 69 6D 20 42 72 65 69 73 67 61 **74**

Die Basisfunktion errechnet die neuen Bestimmungsdaten wie folgt:

Hash Constant (Ck) =	<b>1681</b>
Summe (ai+1) =	<b>3992</b>
Summe (ai+1)*pi =	<b>86518</b>
Positionsgewichteter Wert (Hk) =	<b>6797070</b>
Zwischenwert (Hp) =	<b>588068903247</b>
Gesamtwert (Hp+Hk) =	<b>588075700317</b>

**Variante = 6**

**Alpha = 238**

**Beta = 60**

**Gamma = 37**

**Delta = 38**

**Theta = 15**

Die **>Hash Funktionsfolge<** umfasst 247 Ziffern im Zahlensystem zur Basis 77

CèeeqiaQcWäYdYQ18aaWm1VLf6ZcLâR81xsAb223xêKV2k9gly#&EjC1àcy&D3Z@4ëS3FP  
âXæ4BWtvb4DçL6x3êLN&I5qDyë55FJ7bf1il4IL4âêSMh6HAj9G6VYPeO1âwPàP42âmpi7  
GâNHä6oyDI073çxsM7DHWWà86Væhá9KbU6k2hzãOX8dâmnë98ã6XZ2&ç@ëa5ãWWawAUcE  
ê39au1kBA8@qèzBRvRvYAYRÉE#A6ázàaCQBâêp

Die Variablen sind Ziffern (keine Zeichen) im Zahlensystem zur **Basis 77**

In Ausschnitten zeigt sich die Berechnung der Ziffern wie folgt:

char	pi	Hk	(ai+1)*pi*Hk	Si	base 77			
	(ai+1)	(ai+1)*pi		pi+code+r				
<b>B</b>	67	11	737	6797070	5009440590	13	5009440603	<b>1àcy&amp;D</b>
<b>r</b>	115	12	1380	6797070	9379956600	14	9379956614	<b>3Z@4èS</b>
<b>a</b>	98	13	1274	6797070	8659467180	15	8659467195	<b>3FPäXæ</b>
<b>u</b>	118	14	1652	6797070	11228759640	16	11228759656	<b>4BWtvb</b>
<b>n</b>	111	15	1665	6797070	11317121550	17	11317121567	<b>4DçL6x</b>
<b>b</b>	99	16	1584	6797070	10766558880	18	10766558898	<b>3êLN&amp;I</b>
<b>ä</b>	133	17	2261	6797070	15368175270	19	15368175289	<b>5qDyé5</b>
<b>r</b>	115	18	2070	6797070	14069934900	20	14069934920	<b>5FJ7bf</b>

Die Rückrechnung auf dezimale Zahlen durch MODULO 256 beginnt beim Parameter **Variante = 6**:

.....**iaQcWäYdY**.....

Ziffern	dezimal	MODULO	Element
Basis 78		256 - Theta	
<b>iaQ</b>	270530	194	15 <b>179</b>
<b>aQc</b>	221090	162	15 <b>147</b>
<b>QcW</b>	161180	156	15 <b>141</b>
<b>cWä</b>	233756	28	15 <b>13</b>
<b>WäY</b>	200026	90	15 <b>75</b>
<b>äYd</b>	416403	147	15 <b>132</b>
<b>YdY</b>	209932	12	15 <b>253</b>

### BASIS-VARIATION (256 Elemente)

Verteilung der Elemente

**179 147 141 013 075 132 253** 067 230 047 102 003 205 113 018 030  
 060 061 137 076 089 103 181 116 203 014 154 229 155 122 225 227  
 024 158 130 011 148 182 119 134 017 180 209 064 081 031 218 107  
 015 176 169 133 143 210 098 242 039 065 117 069 172 090 232 079  
 238 086 219 144 123 084 108 145 223 138 063 234 125 020 135 082  
 044 220 070 131 235 115 170 243 120 114 036 091 106 062 196 188  
 197 207 048 033 032 104 087 136 160 127 251 066 233 194 193 046  
 088 051 187 037 029 034 191 093 226 228 245 139 056 252 092 080  
 231 254 094 109 095 035 118 078 216 000 001 204 002 142 006 055  
 244 022 128 105 068 167 004 248 085 052 213 121 071 043 005 072  
 124 171 007 077 019 165 111 236 146 240 208 183 126 129 110 206  
 053 025 074 237 166 239 140 211 246 186 241 151 168 153 221 073  
 038 083 157 247 096 163 057 149 249 150 152 156 097 040 008 159  
 099 198 161 162 100 199 021 101 164 026 212 023 009 041 255 042  
 016 173 058 028 250 112 178 214 174 175 185 177 027 184 189 195  
 010 217 192 190 200 201 202 215 054 045 059 049 222 224 012 050

## CypherMatrix (16x16) abgeleitet aus der BASIC-VARIATION (256 Elemente)

1	71	DA	52	58	16	4A	A2	C8	67	62	F3	E2	34	F1	17	DE	16
17	7A	E8	BC	E7	AB	9D	1C	4B	B6	6C	88	D8	F0	98	B1	CD	32
33	1F	87	2E	F4	19	A1	BE	59	D2	AA	5D	55	BA	D4	31	9B	48
49	5A	C4	50	7C	53	3A	0D	94	54	57	4E	92	96	B9	03	51	64
65	14	C1	37	35	C6	C0	4C	8F	73	BF	F8	F6	1A	3B	E5	AC	80
81	3E	5C	48	26	AD	8D	0B	7B	68	76	EC	F9	AF	66	40	7D	96
97	C2	06	CE	63	D9	89	85	EB	22	04	D3	A4	2D	9A	45	6A	112
113	FC	05	49	10	93	82	90	20	23	6F	95	AE	2F	D1	EA	E9	128
129	8E	6E	9F	0A	3D	A9	83	1D	A7	8C	65	36	0E	75	5B	38	144
145	2B	DD	2A	B3	9E	DB	21	5F	A5	39	D6	E6	B4	3F	42	02	160
161	81	08	C3	3C	B0	46	25	44	EF	15	D7	CB	41	24	8B	47	176
177	99	FF	32	18	56	30	6D	13	A3	B2	43	11	8A	FB	CC	7E	192
193	28	BD	1E	0F	DC	BB	69	A6	C7	CA	74	27	72	F5	79	A8	208
209	29	0C	E3	EE	CF	5E	4D	60	70	FD	86	DF	7F	01	B7	61	224
225	B8	12	6B	2C	33	80	ED	64	C9	B5	F2	78	E4	D5	97	09	240
241	E0	E1	4F	C5	FE	07	F7	FA	84	77	91	A0	00	D0	9C	1B	256

Die folgenden Parameter zur Steuerung von Verschlüsselungen holt das Programm aus der laufenden CypherMatrix:

**Alpha:**  $((H(k) + H(p) \text{ MOD } 255) + 1) = 238$ , legt den Beginn des **Chiffre-Alphabets** von 128 Elementen fest:

1	71	DA	52	58	..	4A	A2	C8	67	62	F3	E2	34	F1	..	..	16
17	7A	E8	BC	E7	AB	9D	..	4B	B6	6C	88	D8	F0	98	..	CD	32
33	..	87	2E	F4	..	A1	BE	59	D2	AA	5D	55	BA	D4	31	9B	48
49	5A	C4	50	7C	53	3A	..	94	54	57	4E	92	96	B9	..	51	64
65	..	C1	37	35	C6	C0	4C	8F	73	BF	F8	F6	..	3B	E5	AC	80
81	3E	5C	48	26	AD	8D	..	7B	68	76	EC	F9	AF	66	40	7D	96
97	C2	..	CE	63	D9	89	85	EB	..	..	D3	A4	2D	9A	45	6A	112
113	FC	..	49	..	93	82	90	..	23	6F	95	AE	2F	D1	EA	E9	128
129	8E	6E	9F	..	3D	..	..	..	..	..	..	..	..	..	97	..	240
241	E0	E1	4F	C5	FE	..	F7	FA	84	77	91	A0	..	D0	9C	..	256

Bestimmte Zeichen (Hex: **00 bis 20, 22, 2C** und weitere) werden ausgeklammert, weil sie in einigen Situationen noch ihre ursprünglichen Aufgaben wahrnehmen (z.B. **1A** =ASCII-26) und die ordnungsgemäße Durchführung des Programms stören.

**Beta:**  $(H(k) \text{ MOD } 169) + 1 = 60$ , bestimmt den Offset, ab dem 63 Bytes für den laufenden **Block-Schlüssel** entnommen werden:

49	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	64
65	14	C1	37	35	C6	C0	4C	8F	73	BF	F8	F6	1A	3B	E5	AC	80
81	3E	5C	48	26	AD	8D	0B	7B	68	76	EC	F9	AF	66	40	7D	96
97	C2	06	CE	63	D9	89	85	EB	22	04	D3	A4	2D	9A	45	6A	112
113	FC	05	49	10	93	82	90	20	23	6F	..	..	..	..	..	..	128

