

# Changing the Start Sequence

(Ernst Erich Schnoor)

In order to demonstrate the sensitivity of the "[Cryptographic Basic Function in Byte Techniques](#)" one **bit** in the last character of the **start sequence** is changed from „0“ to „1“:

Start sequence (old): **Horse racing on the banks of San Sebastian**  
Start sequence (new): **Horse racing on the banks of San Sebastiao**

**n = 6E = 1101110**  
**o = 6F = 1101111**

48 6F 72 73 65 20 72 61 63 69 6E 67 20 6F 6E 20 74 68 65 20 62  
61 6E 6B 73 20 6F 66 20 53 61 6E 20 53 65 62 61 73 74 69 61 **6F**

The Basic Function calculates the new destination Data as follows:

Hash Constant (Ck) = **1681**  
Sum (ai+1) = **3902**  
Sum (ai+1)\*pi = **84250**  
position weighted value (Hk) = **6643512**  
partial interim value (Hp) = **559715886987**  
total hash value (Hp+Hk) = **559722530499**

Variante = **8**  
Alpha = **175**  
Beta = **123**  
Gamma = **189**  
Delta = **155**  
Theta = **25**

The **hash function series** contains 248 digits in number system on base 77

DzNPfgPpgWàFaX01ArDL@1JTh&DbWOJq1êAXpN1æC@æV2G6ãJ82kPH5T2ëw8V234á1GG  
1 4 5àTx3àPqàw46pIZN1Myd17**4ã9BR4nEZe64wJé5D1luTdá57ã&DN5MZOG06Kbchà6Rá2dg**  
**79561h**28Brd7WcfXM763l@i2QáRU@6EJLrd7ZBKjl8tM3YG2p&Häk70vye88wqêo28vgp  
iy8äKäMBA#4nEqBFRGZ5AVNäLX9áROv@Bg04hG

The variables are digits (not characters) in number system on **base 77**

char	pi	Hk	(ai+1)*pi	(ai+1)*pi*Hk	Si	base 77		
(ai+1)	(ai+1)*pi			pi+code+r				
t	117	17	1989	6643512	13213945368	19	13213945387	4âä9BR
h	105	18	1890	6643512	12556237680	20	12556237700	4nEZe6
e	102	19	1938	6643512	12875126256	21	12875126277	4wJé5D
	33	20	660	6643512	4384717920	22	4384717942	1luTdá
b	99	21	2079	6643512	13811861448	23	13811861471	57ä&DN
a	98	22	2156	6643512	14323411872	24	14323411896	5MZOgO
n	111	23	2553	6643512	16960886136	25	16960886161	6Kbchà
k	108	24	2592	6643512	17219983104	26	17219983130	6Rá2dg
s	116	25	2900	6643512	19266184800	27	19266184827	79561h

Reconversion to decimal numbers by MODULO 256 on **base 78**  
at parameter **variante = 8**:

.....pgWàFaX01A.....

digit	decimal	MODULO	element
base 78		256 - Theta	
pgW	313592	248	25 223
gWà	258089	41	25 16
WàF	199773	93	25 68
àFa	396666	122	25 97
FaX	94101	149	25 124
aX0	221598	158	25 133
X01	200773	69	25 44
01A	88	88	25 63

### BASIC-VARIATION (256 elements)

Contracting >Hash function series< to decimal numbers 000 - 255

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



