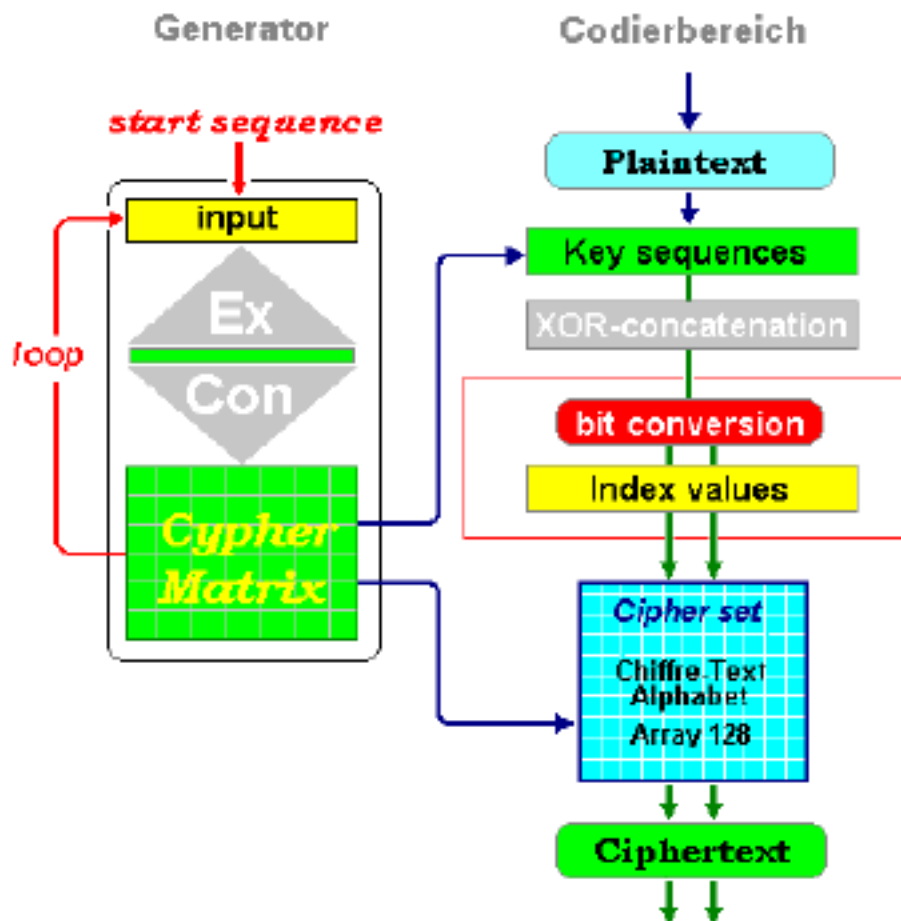


CypherMatrix

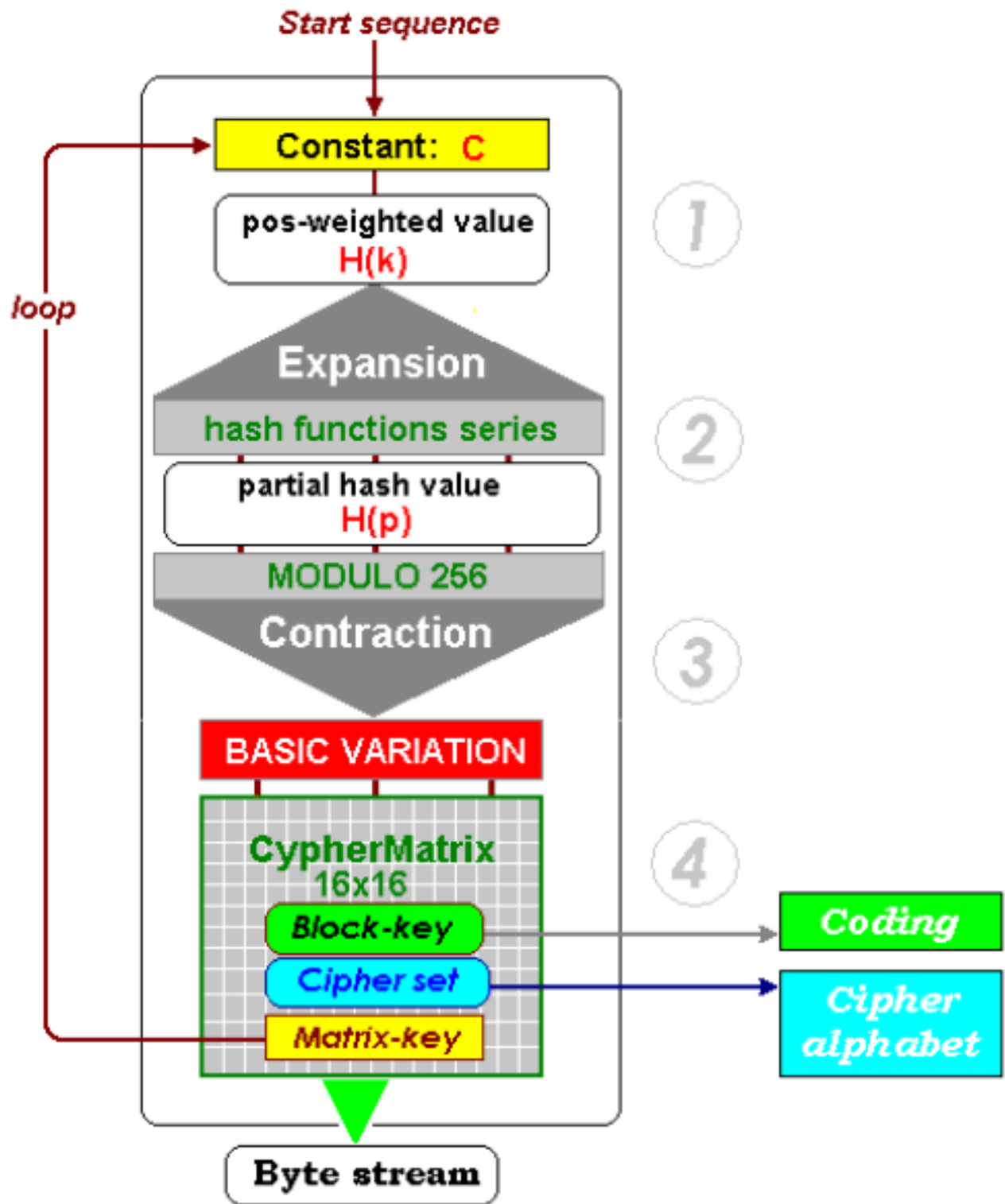
Aufbau des Daten Generators

CypherMatrix arbeitet mit zwei getrennten Bereichen:



Beide Bereiche werden miteinander kombiniert, können aber auch getrennt voneinander eingesetzt werden.

Daten Generator



1

Erweiterung der **Start-Sequenz** zum positionsgewichteten Zwischen-Wert H_k

$$C_k = n * (n - 2) + \text{code}$$

$$H_k = \sum_{i=1}^n (a_i + 1) * (p_i + C_k)$$

2

Hochrechnung der **Start-Sequenz** zur Hash-Funktions-Reihe im Zahlensystem zur **Basis 77 (Expansion)** und Hash-Wert H_p

$$s_i = (a_i + 1) * p_i * H_k + (p_i + \text{code})$$

$$H_p = \sum_{i=1}^n s_i$$

3

Verdichtung der Hash-Funktions-Reihe durch **Modulo 256** zum Array **BASIC-VARIATION (Contraction)**

4

dreifache Permutation der **BASIC-VARIATION** zur CypherMatrix als finaler **Hash-Wert H**

Baron Münchhausen reitet über den Bodensee

$$n = 42$$

$$\mathbf{A} = a(1), a(2), a(3), \dots a(i), \dots a(n)$$

Verknüpfung durch Addition:

$$H(k) = a(1) + a(2) + a(3) + \dots + a(i) \dots + a(n)$$

$$a(i) = a(i) + 1$$

$$H(k) = \sum_{i=1}^n (a(i) + 1)$$

$$H(k) = 4074$$

Der Wert ist zu klein, es müssen weitere Merkmale hinzukommen.

Positionsgewichtung

Jeder Sachverhalt wird eindeutig bestimmt durch die Koordinaten für:

Gegenstand * Ort * Zeit

„Ort“ ist die Position $p(i)$ des Zeichens $a(i)$ in der Start Sequenz \mathbf{A} .

Die Koordinate „Zeit“ ist nicht relevant: $t(i) = 1$

$a(i)$ wird **positionsgewichtet** durch Multiplikation mit der Position $p(i)$

$$H(k) = \sum_{i=1}^n (a(i) + 1) * p(i) * t(i)$$
$$t(i) = 1$$

Ausschluss von Kollisionen durch Hashkonstante $C(k)$

$$\begin{aligned}C(k) &= n * (n - 2) + \text{code} \\C(k) &= 1681\end{aligned}$$

Mit $C(k)$ errechnet sich das partielle Ergebnis $H(k)$ wie folgt:

$$\begin{aligned}H(k) &= \sum_{i=1}^n (a(i) + 1) * (p(i) + C(k)) \\H(k) &= 6935825\end{aligned}$$

Expansion zur Hash-Funktionsreihe (HFR)

Berechnung der Hash-Funktionsreihe und eines weiteren partiellen Zwischenwerts $H(p)$.

Pseudo Code:

```
FOR i = 1 TO n
  S(i) = ( ( a(i) + 1 ) * p(i) * H(k) ) + ( p(i) + code )
  CALL DezNachSystem ( 85, S(i), digit )
  Reihe = Reihe + digit
  H(p) = H(p) + S(i)
NEXT i
```

Das Zahlensystem zur Basis **85** hat folgende Ziffern:

0123456789ABCDEFGHIJKLMN**OP**QRSTUVWXYZ
abcdefghijklmnopqrstu**vwxyz&#@ääääääæçèéëïíî**{|}€

(definiert vom Autor, nicht standardisiert)

Die Hash-Funktionsreihe umfasst 251 Ziffern im Zahlensystem zur Basis 85:

1pu|WY58ëwW7Q3oLhjæVs@xisCyè#6laQQFHbçkaà}1rFnãî1I&jãU1lèääQ1ãdW2H1J
f31€NTCJ2ngY€02zGMçæ2kæjeH2izdPlíijqO3ZR26y3G4ZoL3eà67R420Rtè3uySFO48
6€A1OqZ1á5O8DBg4FDZM84deFâT5I9îJF1kjë2B4ë0€EH58w5iX5zxQNî1@6våZ3un3
Hf6 Pz&TM5æj4fr64€ëAd6àG0Cå7LhWqk6jtäyg6xHáKh

Die **Hash-Funktionsreihe** errechnet sich auszugsweise wie folgt:

char	a_i+1	p_i	$(a_i+1)*p_i$	H_k	$(a_i+1)*p_i*H_k$	s_i	Basis85
·
M	78	7	546	6935825	3786960450	3786960458	çkaà}
ü	130	8	1040	6935825	7213258000	7213258009	1rFnãî
n	111	9	999	6935825	6928889175	6928889185	1l&jäU
c	100	10	1000	6935825	6935825000	6935825011	1lèåáQ
h	105	11	1155	6935825	8010877875	8010877887	1ãdW2H
h	105	12	1260	6935825	8739139500	8739139513	1 ZJf3
a	98	13	1274	6935825	8836241050	8836241064	1€NTCJ
u	118	14	1652	6935825	11457982900	11457982915	2ngY€0
s	116	15	1740	6935825	12068335500	12068335516	2zGMçæ
e	102	16	1632	6935825	11319266400	11319266417	2kæjeH
n	111	17	1887	6935825	13087901775	13087901793	2ïzdPI
·
Summe =						606406116520	1puµ7aA

Partielle Hash-Werte als Basis für Steuerungsparameter

Hash Konstante (Ck): $1680 + 1 = 1681$
positionsgewichteter Wert (Hk): **6935825**
partieller Hash-Wert (Hp): **606406116520**
Gesamt Hash-Wert (Hk+Hp): **606413052345**

Daraus gewonnene Steuerungsparameter:

Variante : $(Hk \text{ MOD } 11)+1 = 7$ Beginn Rückumwandlung
 Alpha : $(Hk+Hp \text{ MOD } 255)+1 = 91$ Beginn Chiffretext-Alphabet
 Beta : $(Hk \text{ MOD } 169)+1 = 66$ Offset Block-Schlüssel
 Gamma : $((Hp+Code) \text{ MOD } 196)+1 = 150$ Offset Matrix-Schlüssel
 Delta : $((Hk+Hp) \text{ MOD } 155)+code = 31$ Beginn Bit-Folgen
 Theta : $(Hk \text{ MOD } 32)+1 = 18$ dynamische Zahlenfolgen

Die Expansion stellt eine erste **Einweg-Funktion** des Verfahrens dar.

Verdichtung zur GRUND-VARIATION

Pseudo-Code:

```
FOR k=1 TO 256
```

```
  Zahl = MID$(Reihe, k, 3)           dreistellige Zahl Basis 86  
  CALL SystemNachDez (86, Zahl, Dezimal)   Rückumwandlung  
  Element = (Dezimal MOD 256)           Begrenzung auf 0 bis 255
```

```
Variation(k)=Element           GRUND-VARIATION: 256 Elemente
```

```
IF k>1 THEN
```

```
  n = 0
```

```
  DO
```

```
    INCR n
```

```
    IF Variation(n) = Element THEN
```

```
      INCR Element
```

```
      Variation(k) = Element
```

```
      n = 0
```

```
    END IF
```

```
  LOOP UNTIL n = k-1
```

```
END IF
```

```
NEXT k
```

Entwicklung der Daten

1pu|WY58ëwW7Q3oLhjæVs@xisCyè#6laQQFHbKb.....

Beginn der Rückumwandlung bei: **Variante = 7**

3 Ziffern Basis 86	dezimal	modulo 256
58ë	37744	112
8ëw	65762	226
ëwW	567116	76
wW7	431727	111
W7Q	237300	244
7Q3	54011	251
Q3o	192604	92
3oL	26509	141
oLh	371649	193
...

GRUND-VARIATION (256 Elemente) Verteilung der Elemente

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

Die **Contraction** stellt die zweite **Einweg-Funktion** des Verfahrens dar.

Aus der GRUND VARIATION erzeugt das Verfahren die

CypherMatrix

in drei Schleifen (Permutationen)

Elemente der CypherMatrix sind alle Zeichen des erweiterten ASCII-Zeichensatzes (00 bis 255).

```
k = Alpha                                     Initialisierung
FOR i = 1 TO 16
  FOR j = 1 TO 16
    Matrix$(1,i,j) = CHR$(Variation(k))      GRUND-VARIATION
    INCR k                                    256 Elemente
    IF k > 256 THEN k = 1
  NEXT j
NEXT i
```

```

CypherSet$ = ""
FOR s = 1 TO 3
    FOR i = 1 TO 16
        FOR j = 1 TO 16
            a = i - j
            IF a <= 0 THEN a = 16 + a
            SELECT CASE s
                CASE 1
                    Matrix$(2,a,j) = Matrix$(1,i,j)
                CASE 2
                    Matrix$(3,a,j) = Matrix$(2,i,j)
                CASE 3
                    Char$ = Matrix$(3,i,j)
                    CypherSet$ = CypherSet$+Char$
            END SELECT
        NEXT j
    NEXT i
NEXT s

```

CypherMatrix in drei Schleifen
(Permutationen)

SERIES01.RND

**CypherMatrix (16x16) aus der GRUND-VARIATION
(256 Elemente)**

```

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

```

Hash-value: Line 7 (CM-final hash)

```

3A 2F 37 DE 9F EA 94 C5 C8 6F C2 EF 40 2D 62 F6

```

Die CypherMatrix ist das finale Ergebnis einer Runde und eine eindeutige Abbildung der Eingabe Sequenz. Die Daten der CypherMatrix haben alle Eigenschaften einer dynamischen Hashfunktion .

Geänderte Start-Sequenz

Baron Münchhausen reitet über den Bodensed

e = 0110 0101

d = 0110 0100

Expanding variables to >Hash function series<:
251 digits in number system base 85

1pmgçèà8ëgX{Q33hejàYVYxhWQfèziHLQPq}èçïëmK1rCuâi1lx&m31læ2Pz1ãaBnv1|Vx
081€JàRg2nbá1€2zBWi12ká{Np2iuEOqíèè{3ZKë0e3F}x8L3ewáJ€41i8äV3ur#yf4X0
HTQ1Oo8Nk5N}v6ì4F5iää4dWE&k5l0mëà1kh9îL4êìHf€58milG5zn2&à1@3jLä3ugc|{6
PoZäl5æYmPb64é1áu6à3çác7LUV716ji6Xë6rfjsC

position weighted (Hk): 6934102
Partial hash value (Hp): 605964240623
Total hash value (Hp+Hk): 605971174725

Variante (Hk MOD 11)+1: 11
Alpha ((Hp+Hk) MOD 255)+1: 241
Beta (Hk MOD 169)+1: 33
Gamma ((Hp+Code) MOD 196)+1: 177
Delta ((Hp+Hk) MOD 155)+Code: 131
Theta (Hk MOD 32)+1: 23

Steuerungsparameter aus der ursprünglichen Start-Sequenz

positionsgewichteter Wert (Hk): 6935825
partieller Hash-Wert (Hp): 606406116520
Gesamt Hash-Wert (Hk+Hp): 606413052345

Variante : (Hk MOD 11)+1 = 7 Beginn Rückumwandlung
Alpha : (Hk+Hp MOD 255)+1 = 91 Beginn Chiffretext-Alphabet
Beta : (Hk MOD 169)+1 = 66 Offset Block-Schlüssel
Gamma : ((Hp+Code) MOD 196)+1 = 150 Offset Matrix-Schlüssel
Delta : ((Hk+Hp) MOD 155)+Code = 31 Beginn dynamische Bit-Folgen
Theta : (Hk MOD 32)+1 = 18 dynamische Zahlenfolgen

**GRUND-VARIATION (256 Elemente)
aus der geänderten Start-Sequenz**

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

**GRUND-VARIATION (256 Elemente)
Verteilung der Elemente**

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

**CypherMatrix (16x16) aus der geänderten Start-Sequenz
(256 Elemente)**

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

Hash-value: Line 7 (CM-final hash)

```
0E 9F 92 FA 06 89 CB 22 D6 7D 95 4E 1B E5 2F F1
```

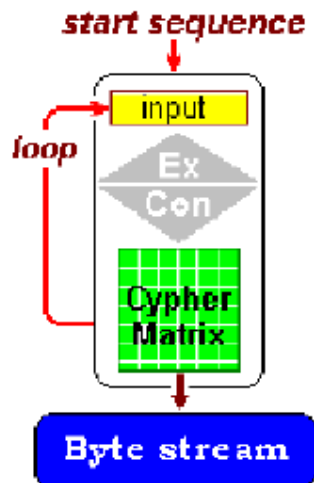
CypherMatrix (16x16) aus der ursprünglichen Start-Sequenz

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

A. Random Byte Generator

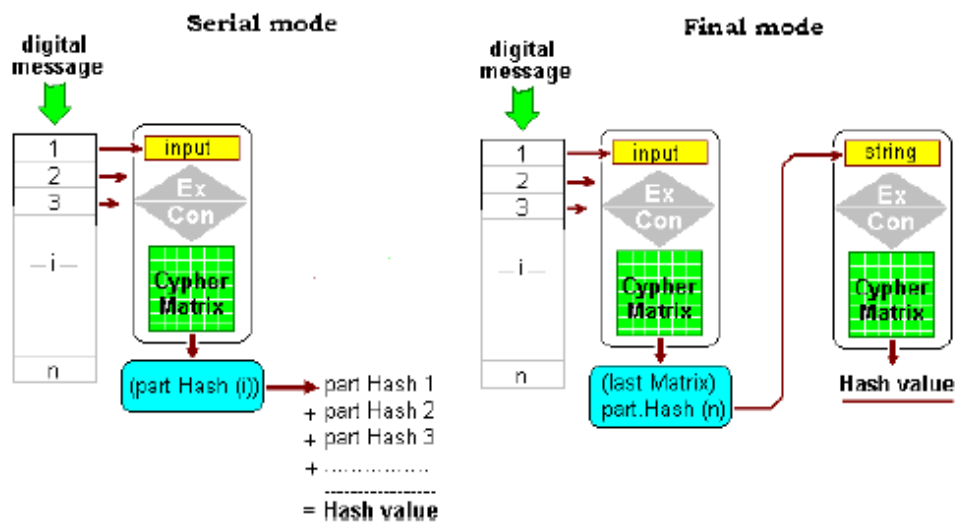
Mit der Start-Sequenz in der ersten Runde wird eine unbegrenzten Bytefolge erzeugt.

Byte Generator



B. Dynamische Hash-Funktion

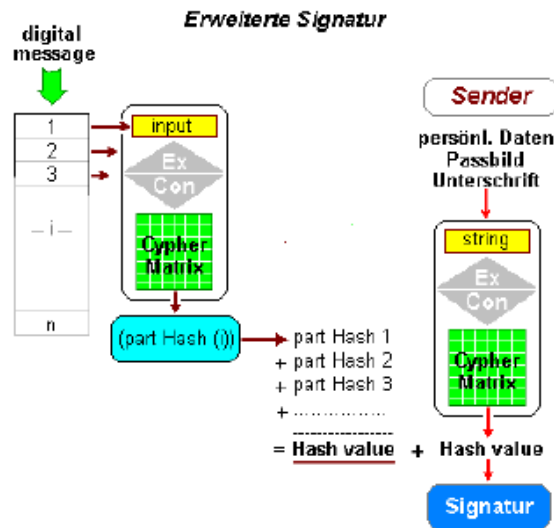
Für jede Runde wird eine eigene CypherMatrix (16x16) als Hash-Wert errechnet. Zwei Methoden sind möglich:



Eine Kompressionsfunktion ist nicht erforderlich.

C. Erweiterte Signatur-Funktion

Anwendung des Generators als Hash-Funktion, sowohl auf eine zu signierende Nachricht als auch auf die persönlichen Daten des Signierenden (Sender) einschließlich Bild und Unterschrift ergeben eine „erweiterte Signatur“.



Ausblick

Das Zusammenwirken von Generator und Codierbereich zur Durchführung von Verschlüsselungen zeigt folgendes Bild:

