

Höherwertige Bit-Umwandlungen

Auszug aus dem Artikel: Cypher's Kern
Abschnitte: Zahlensystem zur Basis 32 und 64
Ergänzung zum Artikel: Bit- und Bytetechnik

(1) Zahlensystem zur Basis 32

Eine **höherwertige** Bit-Umwandlung, und zwar von **8-Bit** auf **10-Bit**-Sequenzen im [Bytesystem zur Basis 10](#), wird im folgenden Beispiel dargestellt:

Zahlensystem zur Basis 32

C 10

In jeder Runde wird zur Durchführung und Steuerung des Programms eine **CypherMatrix** im Zahlensystem zur Basis 32 generiert, entsprechend dem **Bytesystem zur Basis 10**

Basis 32 umfasst die folgenden Ziffern: **0123456789ABCDEFGHIJKLMNQRSTU**
Um **Expansion** und **Verdichtung** zur BASIS VARIATION voll auszuschöpfen, muss die Startsequenz länger sein als 42 Bytes. Für unser Beispiel wird folgende Startsequenz gewählt:

Auf der Fischbachalm gibt es keine Heringe und keine Angelhaken [63 Bytes]

Mit der **Basis Funktion** wird die Startsequenz nacheinander positionsgewichtet, mit der Hashkonstanten **C(k)** multipliziert, zur Hash-Funktions-Reihe expandiert, dann mit **MODULO 1024** zur BASIS VARIATION verdichtet und als **CypherMatrix (GF32^2)** definiert. Das entspricht dem Byte-Alphabet im **Bytesystem zur Basis 10**.

Unser Beispiel liefert für den ersten Durchlauf folgende Bestimmungsfaktoren und Parameter:

Hash Konstante (Ck) : 3843+1=3844
positionsgewichteter Wert (Hk) = 22793584
partieller Hash-Wert (Hp) = 4350474618655
Gesamt-Hash-Wert (Hk+Hp) = 4350497412239

Aus den Hash-Werten gewonnene Steuerungsparameter:

Variante: (Hk MOD 11)+1 = 1 Anfang Verdichtung
Alpha : ((Hk+Hp) MOD 1023)+1 = 474 Chiffre-Alphabet
Beta : (Hk MOD 960)+1 = 305 Block-Schlüssel
Gamma : ((Hp+Code) MOD 944)+1 = 433 Matrix Key

CypherMatrix (GF32^2) im Bytesystem zur Basis 10

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|-----|-----|
| 1 | OA | L5 | 3N | SE | 75 | 3R | T9 | 83 | 6S | 76 | 1V | 8H | Q4 | 08 | M1 | F6 | 71 | DF | C2 | A2 | AG | J3 | IC | 78 | KV | BK | PT | L1 | 2T | B9 | VH | 7S | 32 |
| 33 | MU | LF | RC | PÜ | 2U | NS | 1A | SD | K3 | TD | M9 | JP | GJ | TN | 5B | D1 | 6L | 9B | SI | AJ | VI | 3T | DJ | IS | KI | D5 | 4I | 48 | 8A | SJ | 8K | B0 | 64 |
| 65 | T7 | BO | GU | 79 | 2B | L0 | F7 | UU | OJ | BP | HR | CD | 9R | Q9 | D4 | MN | 1U | GH | UQ | D6 | RN | K2 | N9 | 52 | SF | 4Q | 2Q | AK | P9 | G0 | 20 | NP | 96 |
| 97 | 7J | FS | N6 | 77 | TJ | RS | NM | 7N | C3 | 7B | NT | CO | A3 | KF | S4 | JO | PM | AM | Q3 | 0A | 5H | OE | BE | E2 | MO | CP | M3 | SU | SV | 97 | NI | 5K | 128 |
| 129 | HS | P0 | VV | 2I | UI | T0 | 4M | TK | T8 | 70 | IL | F9 | 16 | R4 | IM | 0F | P8 | RB | U1 | HF | 8B | VB | RI | ET | EU | QK | QF | 9A | T6 | TQ | AN | GT | 160 |
| 161 | 10 | 7A | SL | UJ | HI | DG | AO | 9K | CN | UL | 41 | 13 | 7R | B3 | 53 | KQ | 7M | SK | KS | UK | 6K | DD | CI | VN | M2 | SM | HK | QV | P1 | K1 | QN | Q7 | 192 |
| 193 | F8 | HH | 3S | 1P | QI | JA | 68 | GD | 5V | K9 | A4 | 02 | HO | U4 | BF | FE | U5 | VO | 33 | CQ | LD | EI | 6J | CC | 6P | J4 | UV | M4 | N8 | 45 | JF | 1K | 224 |
| 225 | AQ | AR | 84 | 24 | ME | P2 | G1 | DB | O2 | MS | M5 | UE | 37 | D7 | JH | PQ | TI | FL | MQ | DH | 6A | PJ | QM | GF | 6T | HG | CR | 00 | 8L | FN | NU | HT | 256 |
| 257 | SG | EB | PV | Q8 | SA | C0 | GE | HL | BU | 38 | VP | 2C | L2 | 7K | FU | 7P | PD | AS | 21 | BJ | I0 | S6 | TV | PK | CJ | KJ | OE | BB | OK | CU | HU | 3K | 288 |
| 289 | 66 | 17 | 10 | FG | JC | EH | PN | S7 | 23 | GG | TA | OD | PO | DR | GM | 1N | TU | SN | 49 | 3A | SQ | 94 | FT | 4E | L6 | MG | 9E | K4 | JG | BL | TB | 5A | 320 |
| 321 | CF | CH | RO | 91 | O1 | JL | QA | DL | 8G | RT | PL | SO | AT | N5 | 9N | BN | QU | 0N | 98 | T4 | IB | 5I | 7V | 5C | BC | JK | 3D | TE | T1 | D0 | 51 | E5 | 352 |
| 353 | TO | IP | H3 | JN | AP | LI | P3 | OQ | 5N | CV | 90 | ML | RO | RD | D2 | RE | I4 | 2S | DI | S5 | NC | V8 | 9L | DC | ED | 5J | 7Q | 6R | U2 | R1 | HA | C4 | 384 |
| 385 | 4J | 8E | GV | 6U | UD | 40 | S9 | Q1 | SP | I7 | AD | K6 | TR | QE | D2 | ON | TC | LB | MT | AV | UM | VM | FV | J1 | 87 | 3E | PP | TS | 3F | 8Q | LV | 54 | 416 |
| 417 | NV | 4P | SB | PH | VO | 0B | EA | BM | U3 | N7 | RU | HV | AU | O3 | 6H | DT | LG | G2 | 2H | MK | 1M | 67 | RF | 9Q | 7C | PR | 25 | 8U | A9 | UN | 9I | V6 | 448 |
| 449 | FK | 80 | 3U | QR | NA | I1 | G7 | 9T | G8 | E6 | 95 | L8 | J8 | KA | 7T | PS | VK | FQ | RQ | 1C | N2 | E3 | 36 | QS | IT | UG | MR | 3V | EJ | 0G | 9M | S8 | 480 |
| 481 | L7 | HP | 5T | 4A | N3 | 62 | 3J | 6M | OH | 8I | QJ | 42 | CM | RP | IQ | KE | RR | ID | 34 | 22 | 69 | MF | KL | 07 | BQ | 00 | EV | JJ | 0C | 5L | 0M | G9 | 512 |
| 513 | H2 | 7L | OS | 26 | LN | BR | O5 | NQ | I8 | RJ | 6N | BS | OR | 30 | 27 | DK | RV | NE | A6 | 6B | G3 | QT | U6 | MM | 3Q | 72 | GI | NK | 0V | R2 | LJ | S0 | 544 |
| 545 | 55 | C1 | 8J | 28 | 6O | HQ | PC | N4 | U7 | OL | 8M | HN | 5E | UO | T2 | 01 | OF | MV | 6Q | JQ | 8N | 3L | 7D | CS | DM | I5 | NN | G4 | PI | UH | FA | 2E | 576 |
| 577 | 9F | 74 | NJ | QC | 0H | I9 | 29 | 43 | I2 | OF | B1 | F4 | 2F | A0 | IU | 0H | 6F | KK | B4 | EL | B2 | HJ | TL | B5 | L3 | 1Q | JM | F2 | I3 | Q0 | IJ | 608 | |
| 609 | OI | B6 | D8 | 7U | U8 | BG | MP | P4 | EF | IO | BV | K5 | B7 | O4 | GK | 80 | 81 | DA | 44 | 9P | B8 | 6V | UP | I6 | 1F | OT | 5D | OU | IA | 4C | VT | QO | 640 |

```

641 M6 SS R3 6C AA D3 5M RG L9 BA LA NL KM 8R OV LH 46 FI FH CL LC 99 VF C9 0I SH OM S1 4H UO VJ FJ 672
673 82 LE MI CB TG 03 P7 P5 VL KC BT 8S V1 7E R7 86 T3 85 VQ UR P6 AB L4 D9 RK H1 JO GL US LK VA C5 704
705 A5 PA LL OJ SR IV C7 G5 TP MH BD VR AC O0 QP FM 6G PB U9 RH PE 35 LM JR 2A RL 9C QL 6E TT 70 QQ 736
737 SC CT 4B 04 4T VS 2R PF 2G HM 47 4D UT LR 73 50 C6 3G 09 E0 LO QG HB 0K 88 OB LP 3P ST 7F 4F TF 768
769 89 7G 7H 2J 8P Q5 0L M7 FB 7I DN C8 A7 AH J5 IE 8C LQ CA Q2 LS 2V BH VU 8D N0 LT RM Q6 30 06 1B 800
801 T5 K7 TH MA JS GN UA 5F DE 8F 9D TM AL 05 4G DO J1 KN DP 4K 4L 8T UB 8V BI UC CE H4 90 2K LU FC 832
833 V2 PG CG IF CK 9S QB DQ N1 2L GO V3 DS S2 K8 NB 56 V4 4R 31 DU QD G6 2M NR 92 GA ND 93 V5 S3 NO 864
865 96 DV 9G 07 E1 A8 KG V7 J2 QH E4 R5 00 5P OG E7 E8 NF E9 M8 V9 VC 9H 08 5Q IG R6 06 2N VD VE 4N 896
897 VG 0P 9J IN FD 18 R8 IR OQ R9 OR OS IH 9U OT OU F0 F1 RA 11 9V 12 14 EC H5 1R A1 15 19 II EE EG 928
929 AE EK 1D 4O 1E AF EM 57 KR AI 1G KT 1H EN EO EP 1I MB 1L IJ 1S 1T KB 2O 2P FF IK 4S 32 39 JB 6D 960
961 GP 60 KD EQ 3B J6 3C ER FO 3H 3I 3M ES M0 F3 F5 FP FR J7 4U MC NG 4V JT 50 GB GC GQ 58 MJ 59 GR 992
993 GS 09 NH MD 5G 5R H6 JU 5S 5U H7 OC H8 6I 6L 63 H9 HC J9 HD 64 HE JD OD JE 65 JV K0 KH KO KP KU 1024

```

BlockKey =

TUSN493ASQ94FT4EL6MG9EK4JGBLTB5ACFCHRO91O1JLQADL8GRTPLSOATN59NBNQU0N98

Block 10-bit =

11101111101110010111001000100100011010101110011010010010010001111111010010001110
1010100110101101000001001011101010000100100111000001011101011110101011...

MatrixKey =

LGG22HMK1M67RF9Q7CPR258UA9UN9IV6FK8O3UQRNAI1G79TG8E695L8J8KA7TPSVKFRQ1CN2E336QS
ITUGMR3VEJ0G9MS8L7HP5T4AN3623J6MOH8IQJ42CMRPIQ

ASCII-set = °Qô6Ço:ì;EI×2æô~[êA=Æ%`hšý<ôú,âãf\]ÐÛ□Ó6^§9½ŠãÂsÖS,-yZ

Mit Alpha = 474 wird das erste Chiffre-Alphabet wie folgt aus der CypherMatrix herausgezogen:

Basis Alpha =

UGMR3VEJ0G9MS8L7HP5T4AN3623J6MOH8IQJ42CMRPIQKERRID342269MFKL07BQOOEVJJ0C5L0MG9H2
7LOS26LNBRO5NQI8RJ6NBSOR3O27DKRVNEA66BG3QTU6MM3Q

Alphabet = Ð□Ó6^§9½ŠãÂsÖS,-yZŽ{MdBEİ•ztμ"öF·|úHu×}xG´eîIË]ÆØ~âôb³□¥fJÛ:,äÇ7@Ù
çà,,víœ¶E÷2ÑêN/áoLKO...CÒaæP@^Ô"e c3,ff;wçDA4g`bÈp \$X†‡h!ª%<iáèQ0#

Hexadezimal

```

D0 7F D3 36 88 A7 39 BD 8A E3 C2 73 D6 53 82 96
79 5A 8E 7B 4D 64 42 C9 CF 95 7A 74 B5 22 F5 46
B7 7C FA 48 75 D7 7D 78 47 B4 80 EE 49 CB 5D C6
D8 7E E2 F4 62 B3 81 A5 83 4A D9 3A 2C E4 C7 37
AE DA A2 E0 84 76 ED 9C B6 45 F7 32 D1 EA 4E 2F
E5 F3 4C 4B 4F 85 43 D2 61 E6 50 40 5E D4 94 65
63 33 B8 66 A3 3B 77 E7 44 41 34 67 A8 FE C8 70
24 58 86 87 68 21 AA 89 3C 69 E1 E8 51 30 23 AD

```

ASCII-Alphabet

```

1   Ð □ Ó 6 ^ § 9 ½ Š ã Â s Ö S , -      16
17  y z Ž { M d B E İ • z t μ " ö F      32
33  · | ú H u × } x G ´ e î I Ë ] Æ      48
49  Ø ~ â ô b ³ □ ¥ f J Û : , ä Ç 7      64
65  © Ú ç à // v í œ ¶ E ÷ 2 Ñ ê N /      80
81  á ó L K O ... C Ò a æ P @ ^ Ô " e      96
97  c 3 , f £ ; w ç D A 4 g ` b È p      112
113 $ X † ‡ h !ª % < i á è Q 0 #         128

```

Für die Verschlüsselung verwenden wir die Worte von Hermann Hesse aus der Datei: HESSE.TXT (vgl. Abschnitt 4,b)

Klartext: *Als Siddhartha den Hain verließ, in ...*

```

Hex:      41 6C 73 20 53 69 64 64 68 61 72 74 68 61 20 64 65 6E 20 48 61 69 6E 20 76 65
8-bit:    01000001 01101100 01110011 00100000 01010011 01101001 01100100 01100100 1101000
10-bit:   0100000101 1011000111 0011001000 0001010011 0110100101 1001000110 0100011010
Basis 32: 85          M7          68          2J          D5          I6          8Q
BlockKey: TU          SN          49          3A          SQ          94          FT
10-bit:   1110111110 1110010111 0010001001 0001101010 1110011010 1001001000 0111111101
XOR:     1010111011 0101010000 0001000001 0000111001 1000111111 1101100010 0011100111

```

7-bit: 1010111 0110101 0100000 0010000 0100001 1100110 0011111 1110110 0010001 1100111
 Index: 87+1 53+1 32+1 16+1 33+1 102+1 31+1 118+1 17+1 103+1
 Zeichen: Ö ³ y | w F a Z ç
 Chiffretext: ò³·y|wFªZç"0";æ@LÇ,H^ô,,Óap,,ckT □ äM²i/ž2kÜarb" □ UUS8Iéfj ...

Um die Sensibilität des Verfahrens zu demonstrieren wird ein Bit der Start Sequenz von "0" auf "1" gesetzt, und zwar das letzte Bit im letzten Byte. Im Übrigen bleibt die Start Sequenz unverändert.

Auf der Fischbachalm gibt es keine Heringe und keine Angelhake

n = 11001110
 o = 11001111

Für die um 1-Bit geänderte Start-Sequenz berechnet das Verfahren folgende Bestimmungsfaktoren und Parameter:

Hash Konstante (Ck) : 3843+1=3844
 positionsgewichteter Wert (Hk) = 22797491
 partieller Hash-Wert (Hp) = 4352656566236
 Gesamt-Hash-Wert (Hk+Hp) = 4352679363727

Aus den Hash-Werten gewonnene Steuerungsparameter:

Variante: (Hk MOD 11)+1 = 3 Anfang Verdichtung
 Alpha : ((Hk+Hp) MOD 1023)+1 = 377 Chiffre-Alphabet
 Beta : (Hk MOD 960)+1 = 372 Block-Schlüssel
 Gamma : ((Hp+Code) MOD 944)+1 = 574 Matrix Key

CypherMatrix (GF32^2) im Bytesystem zur Basis 10

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
| 1 | F1 | OQ | FV | 8P | T8 | 4U | FM | LI | 5Q | F0 | HP | KQ | 8D | 5U | K2 | G7 | 2H | 1U | 08 | EJ | 40 | HQ | 9S | 9T | HR | 3L | GA | O2 | 20 | 31 | AK | RK | 32 |
| 33 | 4S | D4 | V4 | TP | H0 | OH | JU | 2U | 5L | 1L | PB | KN | 8H | QC | NL | ND | 2E | PC | RB | Q0 | A4 | 3H | J8 | K9 | D5 | US | 4L | 0P | PO | 50 | QH | 4P | 64 |
| 65 | GQ | RR | 3M | 0S | MP | RC | 3S | SP | CP | 7H | BF | N6 | SJ | D9 | RQ | 89 | V7 | BQ | KI | 6A | G9 | J2 | TC | 66 | CF | SQ | DD | MO | QE | T0 | V8 | 5V | 96 |
| 97 | OI | NT | V2 | 0L | DK | MD | E7 | PK | NU | QB | G4 | QJ | NS | S0 | CQ | OJ | M3 | 9M | 79 | NE | 8K | SG | UE | 6Q | 3V | Q6 | TI | OU | 0U | 06 | G8 | JP | 128 |
| 129 | I5 | NR | RS | NQ | EG | GG | OK | PA | E6 | KP | JM | O4 | UV | TF | GD | 70 | 97 | P3 | OR | H9 | H7 | 8E | IB | VP | IG | 57 | TB | R4 | 3J | 5M | DL | B2 | 160 |
| 161 | 1V | RD | AU | 09 | C0 | TJ | 1C | AS | P4 | KG | EH | H4 | RL | 2R | MK | 48 | 6G | 0J | 10 | IR | 6M | PF | TE | 3F | 0M | FA | DA | IT | IF | 6L | OS | V9 | 192 |
| 193 | 1T | 3N | LP | U4 | FT | HK | CH | 07 | K7 | QK | 7E | 98 | 0N | TG | UT | MJ | 0A | 4Q | CB | F6 | HS | R3 | 2L | J4 | HC | OM | 86 | 1P | N0 | 4D | NO | SE | 224 |
| 225 | 4F | OB | RT | 1Q | ML | EO | E1 | LT | CG | UJ | IU | 5C | FE | L6 | KC | JL | JA | 9I | MG | LD | K3 | RU | KJ | A3 | DT | TK | D6 | DB | M7 | 0T | 30 | T3 | 256 |
| 257 | P7 | L5 | V0 | JN | NH | 8S | 7I | SH | L7 | DG | C2 | AV | M2 | LJ | JO | 8M | 7L | BU | CV | HM | KF | Q4 | 2F | 00 | IC | 19 | HO | 6N | 8Q | E9 | 6J | FU | 288 |
| 289 | 10 | 21 | KA | VH | 6H | JV | H1 | FI | DH | OV | K5 | AH | SA | 1F | 2S | B9 | RP | FJ | 1A | FK | LS | 8U | J0 | G1 | PD | GB | 8N | OE | 3G | VE | P8 | 22 | 320 |
| 321 | BT | AR | 5B | I7 | M4 | 8T | OL | LE | U5 | UN | NI | VM | 9A | 7F | DI | Q7 | 99 | RG | DC | 9E | M5 | NV | EI | 3D | IJ | 12 | QQ | MH | OF | 9Q | V3 | FR | 352 |
| 353 | DM | P0 | QF | H8 | Q5 | 4N | 4K | 60 | EL | VA | 9V | 1R | UU | 2V | DF | ON | VN | 4E | B4 | K0 | JK | 0C | EC | VB | UO | RV | L0 | LO | 4V | ME | L1 | 30 | 384 |
| 385 | SR | FL | PP | B5 | MR | IE | 1B | 1E | MM | 05 | 2P | I3 | 41 | 36 | PG | 3I | 8L | GE | TL | AB | D8 | M8 | 0D | LK | MU | HT | 2I | FF | SD | U8 | OQ | DE | 416 |
| 417 | 04 | 2A | B3 | U6 | U7 | KR | 2T | TN | OG | 1N | 83 | 87 | S3 | TV | PJ | 6R | KH | BE | 42 | 6E | DJ | VO | LG | 11 | KS | 7J | VG | A8 | HU | E8 | FB | HB | 448 |
| 449 | 3K | QD | QM | 9F | 5N | GN | 2N | 0A | UK | J9 | 6I | 25 | 13 | CT | V5 | LH | 80 | SI | S5 | 2D | IH | MI | 46 | L8 | 6P | D7 | T4 | RE | 8V | 4R | JT | EQ | 480 |
| 481 | EA | NM | 6S | 88 | AL | HI | R5 | 90 | RM | 82 | I8 | AN | KD | ID | QN | II | BR | C3 | 7N | TM | J1 | ES | 3B | 63 | FN | P6 | JG | TD | OR | VI | P1 | 0T | 512 |
| 513 | TU | TO | QA | 02 | HV | 1J | JJ | M9 | 9G | 32 | MN | 7P | 0H | SN | VT | 94 | NA | 7A | 33 | 8A | IK | 3A | RH | 0V | 91 | UR | L2 | BA | LR | KO | G0 | 2B | 544 |
| 545 | 03 | U9 | 3C | E0 | PL | A9 | N1 | K6 | CU | N4 | QT | 00 | I0 | 67 | 92 | DQ | 3P | 93 | 84 | JB | RO | 4M | 4B | 35 | 95 | A7 | CE | EV | I1 | MQ | LQ | HD | 576 |
| 577 | 52 | Q1 | O1 | BV | MS | B0 | FG | M6 | RN | 6T | G2 | B1 | 9B | 1S | JH | GC | LA | IN | C1 | DN | FP | HL | 3Q | 7V | 20 | PE | MA | 96 | FO | CJ | Q2 | N2 | 608 |
| 609 | 3E | CN | EP | 1G | 3R | IV | H2 | MT | M0 | 1H | 00 | 08 | 3T | K4 | LL | 8R | O6 | 56 | 2G | S1 | 7K | TH | 8J | U0 | 6U | KT | 3U | RI | 26 | EK | 14 | KB | 640 |
| 641 | 23 | UI | K1 | IL | LU | 05 | 40 | 62 | SF | SB | 18 | HA | DR | 4T | 85 | UM | KE | 74 | 68 | BM | 43 | RJ | CR | 5S | K8 | P5 | IM | H5 | 15 | NC | 9H | PH | 672 |
| 673 | 69 | V6 | UA | SK | G3 | 2Q | I2 | QG | 27 | 34 | PT | TQ | HJ | TR | RA | 0B | S4 | 07 | 76 | L9 | VV | Q0 | 37 | 4C | CK | 71 | 38 | 39 | AT | GF | U1 | KU | 704 |
| 705 | Q8 | A0 | 9C | 16 | DO | 17 | IO | 2C | 78 | MV | L3 | 1D | AQ | KK | AM | E4 | 7U | N5 | CI | 09 | KL | 7R | U2 | VQ | 9D | AA | GK | ER | N3 | H6 | 6V | KM | 736 |
| 737 | G5 | 24 | CL | CS | HE | N7 | 44 | SS | B6 | CM | 5P | 70 | KV | A2 | 45 | UL | 47 | 50 | IP | FQ | EB | 0E | 9J | 2J | 49 | F2 | P2 | G6 | 8S | T9 | 51 | FS | 768 |
| 769 | LM | 5R | F3 | I4 | L4 | 8F | 60 | LB | GH | 2K | 28 | 0F | EM | 4A | I6 | 9U | A1 | I9 | 4G | GI | OC | 4H | 4I | AO | S2 | 53 | DP | VC | TS | H3 | OP | LC | 800 |
| 801 | 4J | 5T | 1M | PI | LF | 8I | QI | NN | NF | 2M | PM | RF | Q3 | A5 | 54 | JC | LN | DS | V1 | 55 | 1I | PQ | 61 | QL | 58 | GR | S6 | 59 | 1K | N8 | S7 | 5A | 832 |
| 833 | ST | D0 | 7M | BG | N9 | SL | DU | S9 | 8B | VD | BS | LV | 6B | GJ | J3 | TT | 6C | CO | SU | DV | NB | QP | T1 | VF | 64 | P9 | OD | VJ | 29 | E2 | MF | ED | 864 |
| 865 | PN | PR | QR | GL | QS | PS | SC | D1 | PU | MB | 9N | 7B | NG | 9K | SM | UF | 72 | 5D | Q9 | U3 | PV | 5E | 0G | GM | JQ | IA | QU | SO | QV | EN | GO | R0 | 896 |
| 897 | R1 | EE | M1 | JR | R2 | VK | UB | GP | 7Q | 9L | R6 | R7 | HF | HG | 8G | IQ | VR | IS | 5F | UC | R8 | 5G | 65 | E3 | B7 | 5H | SV | B8 | 0I | C4 | UD | 5I | 928 |
| 929 | BB | R9 | MC | ET | HH | T2 | 5J | NJ | 5K | 6K | 0K | 6D | J5 | 73 | T5 | UG | 6F | 75 | FC | E5 | J6 | J7 | 77 | T6 | VL | 7C | 7D | NK | UH | GS | HN | D2 | 960 |
| 961 | 7G | NP | T7 | 7S | 90 | 7T | UP | VS | TA | UQ | 80 | CC | F7 | JD | VU | 81 | JE | JF | 00 | 8C | 9P | 01 | 9R | 03 | A6 | AC | AD | AE | AF | AG | EU | EF | 992 |
| 993 | AI | D3 | AJ | J1 | AP | FB | CB | BD | JS | BH | BI | BJ | BK | BL | BN | BO | BP | F4 | C5 | F5 | F8 | C6 | C7 | C8 | C9 | CA | CD | F9 | FD | GT | GU | GV | 1024 |

BlockKey =
 K0JK0CECVBUORVL0LO4VMEL130SRFLPPB5MRIE1B1EMM052PI34136PG3I8LGETLABD8M8
 Block 10-bit =
 1010000000100111010000000011000111001100111110101111110110001101111111010100000
 10101110000010011111101100111010101000010001100000111001101101111101...
 MatrixKey =
 MQLQHD52Q101BVM5B0FGM6RN6TG2B19B1SJHGCLAINC1DNFPHL3Q7V20PEMA96FOCJQ2N23ECNEP1G3R
 IVH2MTM01HO0083TK4LL8R06562GS17KTH8JU06UKT3URI
 ASCII-set = Ü°-ÇAÜ`ðEwYa+.qªW□.ù5z□@.Ê&ø"Bân-Ü0{_"ÝÀ1}„µ|P□ô±Àß□~r

Basis Alpha =

UORVL0LO4VMEL130SRFLPPB5MRIE1B1EMM052PI34136PG3I8LGETLABD8M80DLKMUHT2IFFSDU80QDE
042AB3U6U7KR2TTNOG1N8387S3TVPJ6RKHBE426EDJVOLG11

Alphabet = Ø □ , Ÿ Î ; ` > ö 9 e N + . Ö □ f 0 r µ K " È ´ = R ï □ É □ J c Æ Ç œ] · 7 f ç 3 ` n , ï ³ ø !

□ ó ð H > Ê ë , t M V / ¹ W Ô i Ò E # ž á ' ... O Q Ó † © Û Ü Ê ö U 2 g v I X Ž P S { „ ÷ ¶ a k ã ù & p ò " ¾ ° L ? 4 s ì l b × ú - ý \$ ê ì d

Hexadezimal

| | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| D8 | 7F | A0 | B8 | 9F | CE | A1 | 60 | 9B | F5 | 39 | 65 | 4E | 2B | 2E | D6 |
| 59 | 43 | 81 | 66 | 30 | 72 | B5 | 4B | A8 | C8 | B4 | 3D | 52 | EF | 8D | C9 |
| AE | 4A | 63 | C6 | C7 | 9C | 5D | B7 | 37 | 83 | BF | 33 | 91 | 6E | 82 | CF |
| B3 | F8 | 21 | 9D | F3 | F0 | 48 | 3E | CA | EB | 2C | 74 | 4D | 56 | 2F | B9 |
| 57 | D4 | 69 | D2 | 45 | 23 | 9E | E5 | 92 | 85 | 4F | 51 | D3 | 86 | A9 | D9 |
| A7 | A4 | 6F | A2 | 7D | DA | CB | F6 | 55 | 32 | 67 | 76 | 49 | 58 | 8E | 50 |
| 5A | 53 | 7B | 84 | F7 | B6 | 61 | 6B | C3 | F9 | 26 | 70 | AD | F2 | 22 | BE |
| BA | 4C | 3F | 34 | 73 | CC | 31 | 62 | D7 | FA | 97 | FD | 24 | EA | EC | 64 |

Alphabet (ASCII-set)

| | | | | | | | | | | | | | | | | | |
|-----|---|---|---|---|---|---|---|---|---|-----|---|---|----|---|---|----|-----|
| 1 | Ø | □ | , | Ÿ | Î | ; | ` | > | ö | 9 | e | N | + | . | Ö | 16 | |
| 17 | Y | C | □ | f | 0 | r | µ | K | " | È | ' | = | R | ï | □ | É | 32 |
| 33 | © | J | c | Æ | Ç | œ |] | · | 7 | f | ç | 3 | ` | n | , | ï | 48 |
| 49 | ³ | ø | ! | □ | ó | ð | H | . | Ê | ë | , | t | M | V | / | ¹ | 64 |
| 65 | W | Ô | i | Ò | E | # | ž | á | ' | ... | O | Q | Ó | † | © | Û | 80 |
| 81 | Š | ¤ | o | ¢ | } | Ů | É | ö | U | 2 | g | v | I | X | Ž | P | 96 |
| 97 | Z | S | { | „ | ÷ | ¶ | a | k | ã | ù | & | p | ò | " | ¾ | ° | 112 |
| 113 | ° | L | ? | 4 | s | ì | l | b | × | ú | - | ý | \$ | ê | ì | d | 128 |

Chiffre-Text: ° o a ø N ï · È s ¶ Ů i „ 1] v W P e † Û X { È ð „ Î p t / N / Û · □ J ä ÷ Ž ¹ z + " ^ È ^ A " m { l - ...

Vergleichen Sie die veränderten Bestimmungsfaktoren und Parameter mit den obigen Daten und bewerten die Abweichungen.

(2) Zahlensystem zur Basis 64

Eine weitere höherwertige Bit-Umwandlung lässt sich auch mit 12-Bit Sequenzen im Bytesystem zur Basis 12 und dem Zahlensystems zur Basis 64 erreichen.

Zahlensystem zur Basis 64

C 12

Mit der Basis Funktion erzeugt das Verfahren eine CypherMatrix GF(64^2) mit 64x64 Elementen, entspricht dem Byte-Alphabet im Bytesystem zur Basis 12.

Die hierfür erforderlichen unterscheidbaren 4096 Zeichen werden dem Zahlensystem zur Basis 64 entnommen. Jedes Zeichen besteht aus 2 Ziffern. Das System umfasst die folgenden Ziffern:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz&#

Um eine vollständig durchmischte BASIS VARIATION zur erreichen, muss die Start-Sequenz eine Zeichenfolge von mindestens etwa 112 bis 128 Zeichen enthalten. Dazu einige Beispiele:

"Till Eulenspiegel sitzt auf der Zugspitze und raucht Zigarren.
In Hinterzarten steigt er um in den Zug nach Irgendwo" [117 Bytes]

"7 Nordlichter wandern über den großen Belt, weil sie nicht schwimmen können
und ihre wasserdichten Schuhe vergessen haben" [122 Bytes]

Die Sensibilität des Verfahrens zeigt sich, wenn **ein Bit** der Start Sequenz von "1" auf "0" gesetzt wird, und zwar das letzte Bit im letzten Byte. Im Übrigen bleibt die Start Sequenz unverändert.

**Till Eulenspiegel sitzt auf der Zugspitze und raucht Zigarren.
In Hinterzarten steigt er um in den Zug nach Irgendw****n**

o = 1101111
n = 1101110

Hash Konstante (Ck) : 65024+1=65025
positionsgewichteter Wert (Hk) = 1395943891
partieller Hash-Wert (Hp) = 3.88528316976116E+15
Gesamt-Hash-Wert (Hk+Hp) = 3.88528456570505E+15

Aus den Hash-Werten gewonnene Steuerungsparameter:

Alpha : ((Hk+Hp) MOD 3720)+1 = 3530 Chiffre-Alphabet
Beta : (Hk MOD 3968)+1 = 1492 Block-Schlüssel
Gamma : ((Hp+Code) MOD 3872)+1 = 3016 Matrix-Key

Vergleichen Sie die veränderten Resultate mit den obigen Bestimmungsfaktoren und Parameter.

Der Aufbau der umfangreichen CypherMatrix GF(64²) im **Bytesystem zur Basis 12** erfordert viel Zeit, sodass das Verfahren relativ langsam arbeitet, aber dafür absolut sicher ist und nicht gebrochen werden kann. Mit einem Programm dieser Art hätte die "**one-time-pad**" Verbindung zwischen Washington und Moskau während des kalten Kriegs wesentlich kostengünstiger aufgebaut werden können.

Um den Ablauf zu beschleunigen, kann das Verfahren in der Weise modifiziert werden, dass die Erzeugung der **CypherMatrix GF(64²)** auf die beiden ersten Durchläufe beschränkt wird. Die in den weiteren Runden errechneten Bestimmungsfaktoren und Steuerungsparameter werden dann auf die **CypherMatrix** des zweiten Durchgangs bezogen. Bei einem Umfang von 4096 Elementen bleibt eine ausreichende Vielfalt an Variablen erhalten. Die Sicherheit des Programms wird nicht geschmälert.

Wege zu den Originaldateien: telecypher.net/CYPHKERN.HTM
telecypher.net/Bytetechnik.pdf

München, im April 2010

**Copyright (c)
Diplomkaufmann
Ernst Erich Schnoor**
