

# Higher Level Bit Conversion

Extract from Article: Cypher's Core  
Sections: Number System on Base 32 and 64

## (1) Number System on Base 32

A **higher level** bit-conversion from **8-bit** sequences to **10-bit** sequences (in [Byte system on base 10](#)) is shown by the following example:

Zahlensystem zur Basis 32

C 10

To achieve course and control of the program in each cycle a **CypherMatrix (GF32<sup>2</sup>)** in number system on base 32 is generated. Number system on base 32 comprises the following figures:

0123456789ABCDEFGHIJKLMNQRSTU

In order to optimize **Expansion** and **Contraction** for creating BASIC VARIATION the start sequence has to be longer than 42 bytes. For our example we choose the start sequence:

**Sven Hedin is sailing around the Northpole in a green nutshell** [63 bytes]

The **Basic Function** processes the start sequence successively by position weighting, multiplying with hash constant **C(k)**, expanding to Hash-Function-Series, then contracting by **MODULO 1024** to BASIC VARIATION and finally fixing as **CypherMatrix (GF32<sup>2</sup>)**. First cycle serves with following destination factors and parameters:

hash constant C(k) = 3843+1=3844  
position weighted value H(k) = 22835519  
partial hash value H(p) = 4350508904364  
total hash value H(k)+H(p) = 4350531739883

Variante: (H(k) MOD 11)+1 = 4 begin contraction  
Alpha: ((H(k)+H(p)) MOD 1023)+1 = 330 cipher alphabet  
Beta: (H(k) MOD 960)+1 = 960 block key  
Gamma: ((H(p)+Code) MOD 944)+1 = 62 matrix key

CypherMatrix (GF32<sup>2</sup>)

1	98	PU	D4	UP	1M	CM	70	JB	R2	VK	ED	M9	7N	V2	DS	94	T5	I7	M0	EE	O3	8P	U4	6R	VV	FA	8J	D8	00	6M	65	R4	32
33	9R	ST	0D	0S	KM	U7	37	PL	I8	U8	D3	LH	FN	66	IH	Q7	PE	U9	IB	39	K8	9J	6U	VI	P0	CG	DC	KI	3K	RE	NQ	U5	64
65	L8	ES	EV	4G	EM	LF	VU	47	07	3Q	TN	SP	IT	V4	7S	JF	OV	MG	2C	U6	27	FE	V7	DQ	TK	H7	U1	JR	VQ	R6	J7	L2	96
97	C6	2S	F0	C4	V3	5Q	30	38	5R	1E	B6	DM	OS	QH	4N	91	6K	GQ	BS	GG	50	VB	TO	I9	VP	QT	KE	N4	NV	6L	3A	RH	128
129	9Q	5H	V8	EN	UN	JN	UH	JC	D5	BH	TD	OQ	AQ	GT	08	FR	6T	SH	IC	TH	EB	A3	SV	P4	HP	EO	28	CP	EG	ML	EU	ID	160
161	PJ	Q2	D1	E1	2B	K4	G6	61	HD	OU	AI	QI	HQ	7P	P1	EH	7G	BK	9S	SN	OB	9H	VD	LD	3B	75	F4	P8	FS	10	2I	OI	192
193	NE	64	D6	PB	1P	BV	F7	HK	FJ	1Q	MF	8K	DF	SD	H6	DP	00	UO	FO	QA	SJ	5P	GB	MR	3S	8U	JS	CH	QO	3R	7U	7O	224
225	L3	6A	CK	83	O4	I0	A8	3F	J1	S2	AK	NJ	OQ	SE	F8	EP	00	EL	NU	QA	33	OV	7I	B8	QF	G7	EQ	K0	13	JT	BA	CC	256
257	D7	AU	DN	D2	LV	UA	GJ	OL	PR	MT	9K	BD	9I	MB	80	UQ	BO	UB	JJ	IJ	6V	BC	05	A1	MK	95	D9	2H	3D	L5	B9	FB	288
289	FC	20	31	86	TT	Q8	DO	PQ	B4	RT	ER	VA	85	2T	ET	G1	M2	79	7T	KJ	1T	FP	PD	29	0B	J1	60	RI	1L	M5	FU	I6	320
321	60	N0	NO	T4	MP	J5	S0	F1	09	VC	F5	IN	25	CN	IO	TB	7V	15	IL	51	DT	71	HR	AF	CB	O2	P7	V9	F2	FT	1N	P2	352
353	BI	I2	3H	VT	19	AL	SS	UI	RV	A4	H0	1R	KF	BE	GU	5L	55	62	1D	UR	5V	DA	81	1F	US	SF	GF	VS	3N	9L	B5	2V	384
385	9C	BU	GA	BT	BN	GR	N1	IA	UL	CL	PC	UU	S7	CO	V5	0G	DR	3V	ND	GE	F3	2A	UC	OD	SK	74	HN	Q1	8H	M7	N5	N6	416
417	ON	S3	7J	A2	9M	KK	P6	IR	BB	AE	IS	CO	2K	IQ	04	A7	KB	IE	EA	6J	V6	MO	UV	5M	JO	AS	A6	II	L4	E3	KD	IF	448
449	P3	EC	AV	57	CQ	JK	5G	K1	MN	AA	IG	LE	LM	8V	CR	MQ	C1	5T	L7	82	G8	LB	P9	QB	30	5N	12	N3	FK	OH	HL	BL	480
481	AH	J3	F6	A5	TV	GD	QP	O5	8R	DU	VJ	K5	PM	Q6	I4	IK	C2	AR	3E	LO	7F	OU	84	OT	1G	87	8G	MJ	G9	K6	UT	KC	512
513	E8	6S	M3	P5	SC	H8	5A	DB	3L	MH	QM	72	AC	BR	9T	RJ	88	EF	V1	HM	RA	FV	MM	0P	45	40	IP	G4	MS	BM	Q9	9F	544
545	SQ	JG	1H	N2	F9	LS	IU	40	SI	2J	O7	2L	PV	LA	90	PA	FD	HO	O1	BF	LQ	MU	S9	A9	NF	3T	HS	DD	RQ	T0	BP	C3	576
577	2R	TG	RU	5S	58	4V	TI	QC	UD	T1	9N	NI	8N	VE	Q4	HT	H9	M8	1S	JU	BG	RC	TE	1V	1I	IM	TP	MC	QD	G0	7K	RR	608
609	BJ	J4	KN	GC	7A	NC	PF	LN	97	OP	50	FL	CI	OR	CS	01	RD	26	QE	HA	3U	C5	4T	PH	JV	HU	KO	TJ	K2	2U	E4	2M	640

```

641 92 K3 VM KP MV 8L KL AD N7 G2 LC SG QQ 9U 0C 89 4P C7 FM GL K7 DV 41 LP G5 OJ UE UJ PG UF RS QR 672
673 TC LI NP O6 99 0I KQ L9 59 9E K9 UM FQ IV HV CU 1U 63 UG CJ J6 GM G3 CT N8 6N BQ 8A 48 C9 PS TU 704
705 J0 8T GH KA 2D ON 8B VF VG J2 LR MD N9 GI 2P 7L 32 C8 CV 8C QJ EI AB 3P O8 1C 96 T6 D0 GK Q5 68 736
737 QS 34 M4 DE GN 14 CA QN UK JP J8 V0 42 TQ U3 LT CD KR 02 8M FF CE CF GO EJ 9A Q0 DG VH 21 DH 73 768
769 JD R3 VL EK MA 7Q VN E0 9B T7 J9 M1 FG O9 8Q VO 76 03 FH 80 DI 0R 6P 67 R5 9V SU 0E 0T KS VR 3C 800
801 PN JA 06 DJ LJ GP 69 JE QG PI 0A JH 3G KG 90 77 0F PK DK DL KT 3M RF NR 0J LG FI GS 4H GV LK OK 832
833 49 0L 43 TR SR JL OM 8D JM PO MI 2E 10 2F H1 11 E2 TL HB U2 KH 16 R7 JQ L6 E5 35 H2 E6 17 5U 44 864
865 3I 6B 1J B7 E7 PP QK 4Q 93 6Q H3 E9 H4 52 18 TS KU 1A QU KV NA OC 78 3J RK A0 5I 1B H5 1K L0 22 896
897 L1 HC HE TF 23 AT HF 24 HG 7B SL LL TM HH AG T2 PT I1 H1 2G HJ I3 NB I5 LU Q3 QL M6 ME 2N NG NH 928
929 6C NK QV AJ R0 NL 7R R1 NM 7H NN AM SO OE 9P 2O NS 46 7C NT R8 OF 2Q 36 OK OG 6D OH R9 4A OM OO 960
961 RB RG 4B RL 8S RM SM RN RO 4C 4D RP S1 T3 6E S4 S5 4E 9D S6 S8 SA 4F 8E 8F SB 6F T8 8I T9 TA AN 992
993 4I U0 4J AO 4K 4L 4M 4R 4S 4U 53 54 56 5B 5C 7M 5D 5E 5F 5J 5K 6G 6H 6I 7D 7E B0 9G AP B1 B2 B3 1024

```

**BlockKey**

OORBRG4BRL8SRMSMRNRO4C4DRPS1T36ES4S54E9DS6S8SA4F8E8FSB6FT88IT9TAAN4IUO

**Block 10-bit**

```

110001100011011010111101110000001000101111011101010100011100110111011011100101101
101110111110111100000100011000010001101110111100111100000011110100011001

```

**MatrixKey**

RENQU5L8ESEV4GEMLFVU47073QTNSPITV47SJFOVMG2CU627FEV7DQTKH7U1JRVQR6J7L2C62SF0C4V35  
Q3O385R1EB6DMOSQH4N916KGQBSGG50VBTOI9VPQTKEN4

ASCII-set = núÄ`Üß □ Ö p+ z .™] äüöDLÆGîç °´ 'Á{úfgç†\à,,ã°xh». f¶Q-!Ô

Alpha = 330 defines the offset of extracting the first **Cipher-Alphabet** (array of 128 characters) out of the current **CypherMatrix**:

**Base Alpha**

VCF5IN25CNIOTB7V15IL51DT71HRAFCBO2P7V9F2FT1NP2BII23HVT19ALSSUIRVA4H01RKFBEGU5L556  
21DUR5VDA811FUSSFGFVS3N9LB52V9CBUGABTBNGRN1IAUL

**Alphabet**

âWEX«□%U;½á;O<'éâý7"rBqpb)VæÖ□D<□nµ¥Ä¿ª/üw5e\_,~}xãJ•.‡€æ»□íäKÌ"ç8AÇèêfóC6-&[kN~TZG  
EPÊÓèØ¶y]FR¤Ã□Q#Í`\$št,×LS®·>Ú,,¾"-\*Ma, \$îô9u

**Hexadecimal**

```

EC E5 57 45 97 58 AB 7F 25 55 A1 BD E1 3B 4F 8B
27 E9 E2 FD 37 22 72 42 71 FE 29 56 9C D2 7F 44
3C 8F 6E B5 A5 C2 2D BF AA 2F 90 FC 77 35 65 5F
2C 7E 7D 78 E3 4A 95 2E 87 80 E6 BB 81 ED E4 4B
CC 94 E7 38 41 C7 E8 EA 83 F3 43 36 96 26 5B 6B
4E 5C 98 54 5A 47 8C 50 CA D3 EB D8 B6 79 5D 46
52 A4 C3 8D 51 23 CD 60 A7 9A 74 82 D7 4C 53 AE
B7 9B DA 84 BE A8 AC 2A 4D 61 B8 24 EE F4 39 75

```

**ASCII-Alphabet**

```

1  ì  à  W  E  -  X  «  □  %  U  ;  ½  á  ;  O  <  16
17  '  é  â  ý  7  "  r  B  q  p  )  V  æ  Ö  □  D  32
33  <  □  n  µ  ¥  Ä  -  ¿  /  □  ü  w  5  e  _  48
49  ,  ~  }  x  ã  J  •  .  ‡  €  æ  »  □  í  ä  K  64
65  Ì  "  ç  8  A  Ç  è  ê  f  ó  C  6  -  &  [  k  80
81  N  \  ~  T  Z  G  Æ  P  Ê  Ó  è  Ø  ¶  y  ]  F  96
97  R  ¤  ã  □  Q  #  Í  `  $  š  t  ,  ×  L  S  ®  112
113  ·  >  Ú  ,, ¾  "-  *  M  a  .  $  î  ô  9  u  128

```

For encryption purposes we take words of John Steinbeck from the file "CANNERY.TXT" (see sector 4,b)

Plain text: *The WORD is a symbol and a delight ...*

```

Hex:      54 68 65 20 57 4F 52 44 20 69 73 20 61 20 73 79 6D 62 6F 6C 20 61 6E 64 20 61 8-
bit:      01010100 01101000 01100101 00100000 01010111 01001111 01010010 01000100 00100000
10-bit:   0101010001 1010000110 0101001000 0001010111 0100111101 0100100100 0100001000 base
32: AH      K6      A8      2N      9T      94      88      39
blockkey:OO      RB      RG      4B      RL      8S      RM      10

```

```

bit:      1100011000 1101101011 1101110000 0010001011 1101110101 0100011100 1101110110
XOR:      1001001001 0111101101 1000111000 0011011100 1001001000 0000111000 1001111110
7-bit:    1001001 0010111 1011011 0001110 0000110 1110010 0100100 0000011 1000100 1111110
index:    73+1    23+1    91+1    14+1    6+1    114+1  36+1    3+1    68+1    126+1
cipher:   ó      B      Ø      O      «      Ú      ¥      E      A      9
Ciphertext:  óBØO«Ú¥EA9u,-Fè'u/ÄP`OÇ"wk³N×W~t-M#_□ó~@žª":~Ä I"Qø;□$OÖi;{1>-Öª □;-R?

```

In order to demonstrate the **sensibility** of the procedure we change one bit from "0" to "1" namely the last bit in the last byte of the start sequence. All other characters remain unchanged.

### Sven Hedin is sailing around the Northpole in a green nutshelm

```

l = 1101100
m = 1101101

```

```

hash constant C(k) = 3843+1=3844
position weighted value H(k) = 22839426
partial hash value H(p) = 4352692130307
total hash value H(k)+H(p) = 4352714969733

```

```

Variante:      (H(k) MOD 11)+1 = 6          begin contraction
Alpha: ((H(k)+H(p)) MOD 1023)+1 = 868      cipher alphabet
Beta:         (H(k) MOD 960)+1 = 67        block key
Gamma: ((H(p)+Code) MOD 944)+1 = 389      matrix key

```

#### CypherMatrix (GF32^2)

1	I2	1T	LS	IA	SO	JU	1F	IF	B2	VV	PR	2E	N4	S1	V2	4T	FK	MN	RH	K8	T1	11	AJ	6M	HN	MG	IQ	5I	OD	IR	ON	6C	32
33	1S	GE	EI	T6	K3	SI	L8	KO	B3	V9	3J	M0	4D	8F	AU	QI	9G	II	RE	L7	L6	LL	OI	QR	DT	CG	AO	G1	IB	K4	3E	C0	64
65	37	8D	E5	BB	AV	7N	4N	DU	7B	CJ	49	8C	RC	JV	T9	5T	K6	K1	GF	6R	VT	42	4F	GH	OE	JJ	5D	E6	T3	VQ	I6	CC	96
97	NT	2I	JO	90	DS	TG	FR	DQ	G5	OO	EO	VC	J1	56	PA	8U	5K	T4	IJ	1M	JS	OU	4U	QB	3I	JR	P2	OV	FJ	IU	OR	QM	128
129	IO	LN	C8	M1	QJ	T7	Q8	O7	PI	TB	7L	QV	VU	4E	SA	SK	KQ	QU	JQ	U5	FS	LM	IN	NK	90	I7	TK	6N	9U	DN	D3	EJ	160
161	B1	CP	MA	8P	SD	R3	4P	VK	JP	9H	23	H5	2P	PD	BC	S3	FM	P0	PS	BT	3G	KD	JD	0F	O0	IP	6I	CR	47	58	93	U4	192
193	7K	9S	P4	3P	13	LD	1B	AK	7R	JC	UV	T0	7I	SS	QS	IC	PG	6F	MT	9B	57	GJ	QD	I1	9I	6D	96	FE	T8	72	FT	KB	224
225	ID	J3	1K	4G	G9	Q1	1J	B0	I9	9J	R0	9C	GG	5M	A4	GM	PT	H7	92	L1	4H	C5	LV	F9	9T	Q4	9R	D7	9K	5R	FC	IO	256
257	4J	N5	RT	E0	CM	PV	78	1H	MI	RO	J9	VR	I3	7M	C3	P5	91	6L	9D	3T	40	DC	8V	2F	PJ	0N	55	SJ	CU	BV	E7	3D	288
289	HU	HV	60	CH	UJ	EM	7U	2R	ST	Q2	DM	OA	00	38	1E	EH	ED	RI	L4	9A	FV	1L	L5	FL	5F	HO	HK	00	CA	EE	CK	US	320
321	SV	SM	G6	F3	03	EC	H6	KE	7D	J2	EF	DH	KG	B9	O1	L9	07	67	DV	CD	MV	MJ	TI	N0	ML	0B	76	N3	7H	20	O4	3S	352
353	K0	3C	5H	MB	RN	VS	VB	0L	TV	LU	V5	IG	FN	M2	R9	LA	EG	UC	FU	GD	10	VA	66	HP	BU	94	S7	FP	G2	OM	2L	CI	384
385	25	D1	01	HB	MM	QK	70	9V	IS	F0	VL	FQ	V3	VP	DA	V1	Q3	TE	JE	U9	P7	MR	46	02	4K	S4	A0	RV	KK	LB	U3	15	416
417	2V	9Q	5P	EK	2D	U8	84	5V	A5	6P	DO	JA	1R	2S	7T	UF	I4	1V	68	N7	KL	JF	K2	LH	G0	9P	RJ	VD	BD	A2	98	448	
449	IK	7J	EP	A1	PU	IT	G7	P1	NS	V0	VM	1I	50	3F	MC	AN	CL	8N	EQ	R8	6H	7P	PK	0H	2Q	04	5E	3U	0U	K5	SN	6E	480
481	LC	41	E4	P3	5G	DR	JH	E8	L3	PL	8E	F4	1A	JB	FH	CB	AA	63	3K	JT	CQ	L2	TU	OJ	UI	EA	TS	C1	0S	NL	RJ	H9	512
513	9N	H8	EL	M9	V4	1N	AL	K7	MD	VE	4Q	J0	32	KM	UK	AP	73	2N	UL	Q7	4I	VN	0T	7Q	05	1P	LE	88	HI	A3	TJ	5C	544
545	29	LF	59	85	BR	8B	0Q	69	LG	33	AF	F8	0V	35	E1	BL	74	4L	FO	1Q	M4	AR	RK	AM	K9	LO	PO	T2	MO	IH	4M	NU	576
577	7S	TO	VF	M3	R1	A6	Q6	U0	I8	MQ	LI	Q9	G3	9E	HM	IU	QQ	SE	B7	G4	OR	LJ	KS	LK	LP	CE	SC	51	7V	MP	61	QE	608
609	77	CS	CV	QF	MS	EN	BE	G8	CF	4R	KA	A7	10	65	FF	JJ	8I	43	UN	SP	MU	4C	12	GA	C2	TM	NQ	DK	N1	SB	N6	GB	640
641	4S	V6	5J	2T	18	21	VG	T5	S0	QG	1G	IL	S8	TA	6T	KI	KR	QA	22	RA	TC	TR	6S	O8	H2	7C	60	S9	54	GN	BJ	MK	672
673	AH	ER	E2	24	CN	F1	2G	C4	I5	62	26	A8	GR	SR	9L	LQ	V8	J4	QO	SF	ME	KV	V7	DB	CO	U1	70	19	3R	6G	ES	4V	704
705	SQ	A9	GI	NO	CT	AS	C6	IV	L0	2A	NN	P6	QL	AC	M5	OO	NH	KU	TP	KC	27	TT	HA	E3	ET	JG	PM	KF	M6	J8	D9	VI	736
737	C7	IE	JK	GC	N2	6A	82	NV	KH	C9	LR	LT	Q5	MF	N9	06	QC	64	SU	DD	M7	BH	DG	VJ	QH	IM	28	M8	J5	TD	KJ	2B	768
769	J6	B4	08	Q0	2H	NA	S2	V8	52	GK	NB	RL	KN	TF	14	AQ	6Q	H4	MH	J7	5L	OF	JL	0P	6J	2C	GL	EU	TH	KP	SL	NC	800
801	KT	B5	VO	3L	ND	53	8G	B6	QN	9M	JM	RF	NE	NF	NG	0J	QT	E9	D0	AT	GO	JN	NH	3H	D2	39	8H	EB	BF	B8	80	5A	832
833	EV	7E	D4	4A	8J	RD	NI	TL	5U	NJ	NM	GP	6U	09	44	5B	GS	OG	NP	5N	F2	TN	0A	NR	D5	O2	2J	O3	95	F5	TQ	GT	864
865	F6	GU	OS	F7	0C	O5	50	PB	97	5Q	U2	O6	2K	O9	P8	5S	Q0	3M	OB	P9	PC	GV	2M	OT	QP	OC	OH	D6	OI	R2	U6	R4	896
897	OK	PN	U7	81	R5	0D	6B	SG	UA	OL	R6	OM	UB	HO	PE	PF	PH	AB	PP	UD	6V	AD	DP	D8	FA	BA	DE	PQ	8Q	SH	R7	6K	928
929	OE	RB	AE	20	HC	2U	RG	BG	S5	H1	RM	RP	DF	3N	RQ	RR	0G	RS	S6	71	DI	48	75	99	UE	83	AG	UG	3Q	16	UH	1C	960
961	BI	86	UM	0K	0U	UR	UT	79	UU	9F	7A	83	R7	1D	AI	7F	BK	FG	30	7G	H4	31	34	36	3A	89	HD	3B	30				992
993	BM	3V	BN	40	BO	HE	8A	BP	HF	45	HG	BQ	4B	8K	DJ	8L	FB	BS	8M	DL	FD	FI	80	HH	8R	8S	8T	HJ	HL	HR	HS	HT	1024

#### BlockKey

E5BBAV7N4NDU7BCJ498CRCJVT95TK6K1GF6RVT424FGHOEJI5DE6T3VQI6CCNT2IJO90DS

#### Block 10-bit

011100010101011010110101011111001111011100100101110110111110001110101101100100110  
01000100101000011001101011001001111111111101010010010111011010000110101

#### MatrixKey

MMQK7O9VISF0VLFQV3VPDAV1Q3TEJEU9P7MR46024KS4A0RVKKBUB3152V9Q5PEK0P2DU8845VA56PDOJ  
A1R2S7TUFI41V68N7KLJFK2LHG09PRJVDBDA298IK7JEP

ASCII-set = ÖTø?`à\óúäü`á@C@nÉ'Û†"„,□"«Ä%\_:¹ÔMË¿EÛ.j; \ýÏD?Èç•o,+9símB(TóÛ...

Base Alpha

F70CO55OPB975QU2O62KO9P85SQO3MOBP9PCGV2MOTQPOCOHD6OIR2U6R4OKPNU781R50D6BSGUAOLR6O MUBH0PEPFFPHABPPUD6VADDDP8FABADEFQ8QSHR76K0ERBAE

Alphabet = ç,+ ' ° Â T ( ¼ X v ) , V Y | bÆd7ÇeË □ Ê f Ì . / 1K9ÍM¹¨êj@: `gÔkNZ-^pq...!wy\_ xz{| †á^â\*îPÐ}&Ñ0rÖØÚé2ë#34Ritð`ñ\$ahil5m~□€□, f6,,8‡;%<³iŠµíò<"%=>?@ABC½J~œ

Hexadecimal

Table of hexadecimal values: E7 B8 2B 27 BA C2 54 28 BC 58 76 29 2C 56 59 A6 62 C6 64 37 C7 65 CB 90 CA 66 CC 2E 2F 31 4B 39 CD 4D B9 A8 EA 6A AE 3A 91 67 D4 6B 4E 5A 2D 5E 70 71 85 21 77 79 AF 78 7A 7B 7C 86 E1 88 E5 2A CE 50 D0 7D 26 D1 30 72 D6 D8 D9 DA E9 32 EB 23 33 34 52 EF 74 F0 60 F1 24 61 68 69 6C 35 6D 7E 7F 80 81 82 83 36 84 38 87 3B 89 8B B3 EC 8A B5 ED F2 3C 22 25 3D 3E 3F 40 41 42 43 BD 4A 98 8C

ASCII-Alphabet

Table mapping ASCII characters to Base Alpha symbols: 1 ç, + ' ° Â T ( ¼ X v ) , V Y | 16 17 b Æ d 7 Ç e Ë □ Ê f Ì . / 1 K 9 32 33 Í M ¹¨ ê j @ : ` g Ô k N Z - ^ 48 49 p q ... ! w y \_ x z { | † á ^ â \* 64 65 î P Ð } & Ñ 0 r Ö Ø Ú Ú é 2 ë # 80 81 3 4 R i t ð ` ñ \$ a h i l 5 m ~ 96 97 □ € □ , f 6 ,, 8 ‡ ; % < ³ i Š µ í ò < " % = . ? @ A B C ½ J ~ œ 112 113 í ò . " % = . ? @ A B C ½ J ~ œ 128

Ciphertext: d#hÂ6,ðXi,\*j)ÐadTêf<}ñi¨`w...vd)+@^rÖ¨\$.?h/zlö;ÇÐÁf`zÇ£ëOô|°; fiizV.FoðQëðÊ

Compare the changed destination factors and parameters with the forgoing Data above and valuate the differences. To get an own impression you may download the program CYPHER3B.EXE and try once all by yourself.

(2) Number System on Base 64

Further another higher level bit conversion can be attained by 12-bit sequences (in Byte system on base 12) and number system on base 64.

Zahlensystem zur Basis 64

C 12

The Basic Function generates a CypherMatrix GF(64^2) of 64x64 elements. All necessary 4096 different signs are taken from number system on base 64. Each sign consists of two digits. The system comprises the following figures:

0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz&#

The start sequence must have about 112 up to 128 characters especially to get a completely mixed BASIC VARIATION. For this some examples:

"Sven Hedin is sailing around the North Pole in a green nutshell. In Far Rockaway Beach he changes for the Yellow Submarine" [123 bytes]

"Horse racing on the banks of Clearwaterbay with 7362 blue donkeys and kangaroos which are taken from the island of Spitzbergen" [126 bytes]

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

Encrypting the file CANNERY.TXT with the above start sequence "Sven Hedin ..." the procedure creates in second cycle the following destination factors and parameters:

hash constant C(k) = 65024+1=65025  
 position weighted value H(k) = 1425941158  
 partial hash value H(p) = 3.99835041459442E+15  
 total hash value H(k)+H(p) = 3.99835184053557E+15

Alpha: ((H(k)+H(p)) MOD 3720)+1 = 3095 cipher alphabet  
 Beta: (H(k) MOD 3968)+1 = 679 block key  
 Gamma: ((H(p)+Code) MOD 3872)+1 = 146 matrix key

CypherMatrix GF(64^2) [64x64 elements]

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64				
1	aM	w4	NP	eA	Is	Zr	ot	SI	qU	fc	f6	g8	kC	Rk	hy	ai	..	..	E&	9a	c7	wv	b&	Ir	TF	tW	tk	Al	fr	FX	90	ga	lu	eb	64	
65	VK	dU	On	Bx	94	Ye	u2	5q	ul	&f	kn	14	F2	LZ	IH	&M	..	..	0a	Ic	dV	FQ	Ts	ew	Mp	G8	io	Y8	ny	Vl	IZ	Wm	Gl	GH	128	
129	SS	FZ	8k	KZ	6Y	DH	S&	bl	30	pI	6h	WS	Rl	kz	7b	x1	..	..	EQ	UO	fN	LK	a5	a2	Ga	q2	hm	NO	Ci	25	FE	U4	v3	Ez	192	
193	9P	#T	rm	g4	lO	uI	Og	f7	vc	jJ	6Z	DI	T8	n&	zK	Qb	..	..	BZ	MA	4K	Ku	4o	CB	5T	jp	Kc	VM	9M	kP	Tr	rV	58	fV	256	
257	p0	ge	M9	oY	Xy	rD	vm	nt	pF	Wt	4w	3J	X7	92	lJ	5W	..	..	Hi	iI	&W	dt	Ik	Y4	UD	sK	Su	2z	6c	PG	9V	4C	9z	GQ	320	
321	UB	ra	t5	ld	q3	Ey	wx	bW	gd	Ck	Ob	zI	cX	a1	lq	XZ	..	..	8Q	Nx	Pp	NU	ro	8d	BN	&a	Pz	uT	za	Ox	GE	09	oa	7c	384	
385	OC	d&	Cl	Cx	op	cJ	Ta	BP	9Z	oG	K8	MK	fZ	7k	cE	Pf	..	..	Vs	JC	Rb	5A	TQ	Sk	xV	RQ	Sv	hH	hQ	Ay	QF	pr	dM	Jj	448	
449	PT	CX	5S	mC	7f	i8	hL	l1	c5	78	PD	ya	O1	ko	A7	Fp	..	..	am	r9	ub	Q&	bb	&p	3g	bc	mc	xE	E6	hq	FR	p#	yk	8s	512	
513	0j	j4	AD	js	yV	rt	8W	&9	#h	0q	UC	9I	bX	m5	RS	w2	..	..	OD	eR	hP	dd	EC	5B	lq	I2	Vc	Do	OZ	m9	eC	hz	xo	zo	576	
577	6w	gF	rB	q#	c#	u6	z8	pi	ER	Mm	eY	Jt	aT	T3	S1	RR	..	..	bt	IY	de	Zh	sC	Hf	mJ	Dl	la	xJ	z&	Tp	jG	R8	5l	vr	640	
641	Qs	fX	Qc	DB	fH	hf	Ff	KY	WI	cL	#P	ec	lp	3l	xr	Vt	..	..	ty	ih	3K	Es	18	Xj	xO	JT	Iz	Gp	fd	7Y	&H	HA	pn	HB	704	
705	Rv	Mg	vb	dX	I3	oB	lz	Oe	ho	&g	3L	eJ	8Y	JA	sO	2m	..	..	zf	c&	td	na	aA	Th	Qx	PR	tx	BE	lJ	Mo	Ee	H#	rA	jL	768	
769	K7	NM	Oy	fA	f1	aR	Yx	07	X8	h5	mm	sH	Ve	q0	xK	Hq	..	..	yw	7M	Ie	Ch	fe	8S	yq	aP	j&	lg	3M	hR	sU	P0	fW	6F	832	
833	zv	EP	1b	C2	d4	FP	36	PQ	hj	L0	ZQ	DP	Fx	t6	bx	cy	..	..	mX	kF	Nh	U2	s3	ns	ii	sF	xD	oD	og	Qq	ov	J0	gL	JL	896	
897	cs	pR	Zw	O8	4&	Cj	lZ	vC	&G	bd	aJ	Uo	f#	l3	UE	Pe	..	..	qk	x6	2n	rO	m4	4#	Rd	Xi	5l	GJ	o8	Yr	7x	3N	sg	Ti	960	
961	go	WC	Wn	DG	QQ	uJ	VN	O1	kN	Ln	&K	ly	ln	8p	fk	Y0	..	..	16	oS	28	Ae	U5	L8	aS	Ot	Et	Gi	Ul	AK	WJ	mY	4z	gM	1024	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
3073	EJ	6&	h9	z6	VT	#S	C7	m3	8l	vJ	zW	dZ	zZ	PM	1s	&6	..	..	3s	vq	TV	2b	kD	E7	1z	Xh	vK	2T	cG	jT	Bh	82	nG	10	3136	
3137	TN	B#	Ho	bu	C0	e&	11	12	w6	1h	Xu	yM	Di	5R	QY	xy	..	..	Uz	Xw	w7	fz	Q0	z8	k6	6y	ne	m7	TE	m8	tr	#8	i3	F3	3200	
3201	cu	mE	nX	tt	qZ	Gw	Ov	B4	cQ	d9	Er	i5	wa	X5	Ud	Ue	..	..	nn	Qh	3Y	1N	88	cO	5j	kH	KI	Kr	OU	rE	ZM	B9	kf	bE	3264	
3265	aY	wf	0C	XB	LT	HK	#s	vL	8A	f1	20	EM	WX	5k	QP	uR	..	..	wp	BM	go	#t	iL	8I	Fj	K4	BU	Ja	gP	uU	VI	y3	Lg	3328		
3329	Fv	kw	uW	Bb	ze	KJ	&Q	y4	Lh	S5	Ma	Br	QR	FU	CL	fv	..	..	oL	d8	Sm	YT	1f	xB	40	Tx	cP	6L	i6	q1	vt	aE	2M	Lr	3392	
3393	2h	Bj	XP	y8	V3	y9	F&	10	lQ	kS	To	ZA	Ls	fw	#V	kt	..	..	8K	X0	Kw	wq	kY	u&	Ns	fy	nc	66	2Q	2t	di	Kx	TL	Lz	3456	
3457	n#	WP	yE	Bg	dr	Fa	Bi	w8	#v	gC	Rz	ZN	#x	iA	&R	pd	..	..	iN	I8	QV	pe	6d	67	iZ	lU	P1	YU	#m	mG	VB	gS	v1	&T	3520	
3521	Ty	VC	3a	Bz	wA	v9	z4	2d	4v	F0	Z9	TO	ax	G&	Ky	yG	..	..	D8	Lt	SL	yQ	Hr	pX	yy	bF	#&	21	k8	Nq	N6	CQ	YF	wH	3584	
3585	Td	oA	j0	wg	R5	#2	3F	Iq	Q9	22	YG	5I	VE	mH	Zc	&D	..	..	Iv	yR	8N	CF	q7	2R	QA	ND	wP	#d	&F	Ly	Ph	cU	X1	&c	3648	
3649	QC	Jq	N9	2S	jj	5K	gA	Vk	ZG	dw	qI	J9	gX	dR	yz	ZU	..	..	Nc	P2	5L	&U	x0	6a	Tf	mP	5N	fE	GA	Dc	x2	41	fF	FB	3712	
3713	CW	2e	lI	YV	WR	#n	Sq	VF	fQ	gd	L3	&V	aW	x3	qd	yZ	..	..	FV	6B	RY	q9	iQ	D4	yi	YZ	y1	ZY	FC	qA	Iw	D5	HN	jd	3776	
3777	YH	Qu	VZ	ym	y&	43	z0	45	nB	NH	db	WA	bC	FD	XQ	Jb	..	..	Zt	oy	SJ	qb	gW	ib	ic	kJ	R&	ie	al	dj	oz	P8	YN	R#	3840	
3841	M2	im	&e	&u	b8	HQ	oN	DL	DM	WB	DN	#0	DO	cW	oT	kK	..	..	Y1	#y	6e	03	06	k#	4F	FK	M5	JF	0D	o#	Dw	0E	0G	00	3904	
3905	JG	kW	XC	MC	JP	0T	6g	50	D#	Ze	MD	U1	5P	Nb	5Q	8P	..	..	EA	XH	bs	6s	pQ	6u	XI	S0	10	FN	6z	kc	qv	P5	FO	kd	3968	
3969	ki	p1	NL	Nf	p3	JR	p4	Zu	lG	Fr	Fs	Fw	Ss	G0	GC	Je	..	..	IC	P9	pE	JS	pa	JV	Jf	Zz	ph	Jg	R9	Jm	Nr	Nm	Nn	Nt	4032	
4033	aH	Nu	aI	aK	aZ	N&	O2	O3	ab	ae	qJ	O4	b0	b3	O5	qK	..	..	Sh	Si	r4	bG	bH	bI	bJ	bK	bL	bM	bV	bK	eH	eI	eL	eM	4096	

The procedure works in two different modes:

Parameter **alpha** fixes an offset in the current CypherMatrix (4096 elements) from where **256 characters** are taken and stored in a separate cipher-alphabet. This alphabet changes with each new plaintext block of 84 characters. The ASCII-value (index) of a plaintext character gets the concerning character from the cipher alphabet and combines it to the encrypted cipher text.

As second mode the program first changes **84 8-bit** plaintext sequences into **56 12-bit** sequences which are XOR concatenated with block key sequences of equal length (**dynamic one-time-pad**). Then this bit series are divided into **96 7-bit** segments which get the corresponding cipher characters from the **cipher alphabet** (array of 128 elements) and form the cipher text.

The **sensibility** of the procedure will be shown when only one bit is changed from **"1"** to **"0"** namely the last bit in the last byte of the start sequence. All other characters remain unchanged.

**Sven Hedin is sailing around the Northpole in a green nutshell.  
 In Far Rockaway Beach he changes for the Yellow Submarind"**

e = 1101101  
d = 1101100

hash constant C(k) = 65024+1=65025  
position weighted value H(k) = 1506022709  
partial hash value H(p) = 4.47263744599346E+15  
total hash value H(k)+H(p) = 4.47263895201617E+15

Alpha: ((H(k)+H(p)) MOD 3720)+1 = 288 cipher alphabet  
Beta: (H(k) MOD 3968)+1 = 54 block key  
Gamma: ((H(p)+Code) MOD 3872)+1 = 84 matrix key

Compare this results with the destination factors and parameters above.

Mounting the extensive CypherMatrix GF(64<sup>2</sup>) of **4096 elements** requires much time thus the program works relatively slow, but in return due to the feature of bit conversion the procedure is absolutely secure and unbreakable. Whith such a program the "**one-time-pad**" connection between Washington and Moscow during the cold war could have been managed with much less costs.

Speeding up the procedure can be achieved when generating of **CypherMatrix GF(64<sup>2</sup>)** is confined to the first two cycles, both. The calculated destination factors and control parameters concerning further cycles are related to the **CypherMatrix** of the second cycle. The huge range of 4096 elements maintains a sufficient variety of variables. Security of the program is not reduced, at all.

Way to the original article: [telecypher.net/CORECYPH.HTM](http://telecypher.net/CORECYPH.HTM)

**Munich, in August 2009**

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

---