Handycipher

1. Introduction

Handycipher is a low-tech, randomized, symmetric-key, stream cipher, simple enough to permit pen-and-paper encrypting and decrypting of messages, while providing a significantly high level of security by combining a simple 31-character substitution cipher with a 3,045-token nondeterministic homophonic substitution cipher. The basic approach of the cipher is to take each plaintext character, convert it to a key-defined pattern of length five and, using this pattern as a template with one to five holes, select certain ciphertext characters from a 5 x 5 key-defined grid. (A more complete description can be found in [4].)

Handycipher is based on a core cipher which operates on plaintext strings over the ordered 31-character alphabet A

A = {A B C D E F G H I J K L M N O P Q R S T U V W X Y Z , . - ? ^}

and generates ciphertext strings over A*, the same alphabet together with the ten decimal digits Ø–9.[1] Some permutation of the 41 characters of A* is chosen as the secret shared key K, say for example,

O N 2 T P 3 F L D S M K Y , 5 A C V E R 7 W I H 4 1 U G 8 . 9 6 Ø ^ ? - Z X Q J B

The 40 non-space characters of K are displayed as a 5 x 8 table, T_K

O	N	2	T	P	3	F	L
D	S	M	K	Y	,	5	A
C	V	E	R	7	W	I	H
4	1	U	G	8	.	9	6
Ø	?	-	Z	X	Q	J	B

A 31-plaintext-character subkey P is derived from K by omitting the decimal digits

O N T P F L D S M K Y , A C V E R W I H U G . ^ ? - Z X Q J B

and is displayed as a substitution table, ξ_P

m:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,	.	-	?	^
ξ_P(m):	13	31	14	7	16	5	22	20	19	30	10	6	9	2	1	4	29	17	8	3	21	15	18	28	11	27	12	23	26	25	24

Then, by referring to T_K and ξ_P, plaintext characters are encrypted into k-tuples of ciphertext characters by means of the following scheme:

> Regarding the first five columns of T_K as a 5 x 5 matrix comprising five rows, five columns, and ten diagonals, each plaintext character m is encrypted by first

---

[1] It's important, of course, to be able to distinguish the digits Ø and 1 from the letters O and I.

expressing $\xi_P(m)$ as a five digit binary number $b_1b_2b_3b_4b_5$ and by using the position of the 1's in this number as a pattern, associating the plaintext character m with a subset of the ciphertext characters comprising a randomly chosen row, column, or diagonal. Then a randomly chosen permutation of that subset is taken as the corresponding k-tuple of ciphertext characters.

For example, the plaintext character I occupying position 19 = 10101 is encrypted into one of the six permutations of one of the twenty 3-tuples

{OCØ NV? 2E- TRZ P7X O2P DMY CE7 4U8 Ø-X OEX NRØ 27? TC- PVZ OR? N7- 2CZ TVX PEØ}

whereas the plaintext character K occupying position 10 = 01010 is encrypted into one of the two permutations of one of the twenty 2-tuples

{D4 S1 MU KG Y8 NT SK VR 1G ?Z SG M8 K4 Y1 DU YU DG S8 M4 K1}

This roughly sketched scheme is now defined more precisely as follows.

2. The Core Cipher

A plaintext message M is encrypted into a ciphertext cryptogram C using a 41-character key K by means of the encryption algorithm E defined as follows:

Core cipher encryption algorithm: C ⇐ E(K,M)

First, omitting ^ the remaining 40 characters of K are displayed as a 5 x 8 table T_K by writing successive groups of eight characters into the five rows of the table.

The first five columns of T_K comprise a 5 x 5 square array (or matrix) M_K and the rows, columns, and diagonals of M_K are designated R_1–R_5, C_1–C_5, and D_1–D_{10}, respectively. We refer to them collectively as *lines*, and call two characters colinear if they lie in the same line. The 15 characters comprising columns C_6–C_8 are said to be *null characters*.

Also, a 31-character *plaintext-subkey* P is derived from K by omitting the ten decimal digits, and a simple (numerical coding) substitution ξ_P is applied, transforming each character m of M into the number $\xi_P(m)$ representing its position in P (i.e., if $P = p_1p_2 \ldots p_{31}$ then $\xi_P(m) = i$ where $m = p_i$).

Then the following three steps are applied in turn to each character m of M.

1. A random choice is made (with equal probability of each of the 20 possible rows, columns or diagonals) between:
   1.1. *Column-encryption*: One of the five columns in M_K, say C_j, is randomly chosen (with equal probability), or
   1.2. *Row-encryption*: One of the five rows in M_K, say R_j, is randomly chosen (with equal probability) subject to the restriction that $\xi_P(m) \neq 1, 2, 4, 8,$ or 16, or
   1.3. *Diagonal-encryption*: One of the ten diagonals in M_K, say D_j, is randomly chosen (with equal probability) subject to the restriction that $\xi_P(m) \neq 1, 2, 4, 8,$ or 16.

2. $\xi_P(\mathtt{m})$ is expressed as a five digit binary number, $b_1b_2b_3b_4b_5$, and if the position of the character $\mathtt{m}$ in $\mathtt{M}$ is an odd number, then
   - 2.1. If 1.1 was chosen in step 1, then for each i such that $b_i = 1$, the i-th element of C_j is chosen, yielding a subset of the five characters comprising C_j, or
   - 2.2. If 1.2 was chosen in step 1, then for each i such that $b_i = 1$, the i-th element of R_j is chosen, yielding a subset of the five characters comprising R_j, or
   - 2.3. If 1.3 was chosen in step 1, then for each i such that $b_i = 1$, the i-th element of D_j is chosen, yielding a subset of the five characters comprising D_j.

   but if the position of the character $\mathtt{m}$ in $\mathtt{M}$ is an even number, then
   - 2.4. If 1.1 was chosen in step 1, then for each i such that $b_i = 1$, the (6-i)-th element of C_j is chosen, yielding a subset of the five characters comprising C_j, or
   - 2.5. If 1.2 was chosen in step 1, then for each i such that $b_i = 1$, the (6-i)-th element of R_j is chosen, yielding a subset of the five characters comprising R_j, or
   - 2.6. If 1.3 was chosen in step 1, then for each i such that $b_i = 1$, the (6-i)-th element of D_j is chosen, yielding a subset of the five characters comprising D_j.[2]
3. The elements of the subset specified in Step 2 are concatenated in a randomly chosen order. If this string, composed of 1 to 5 ciphertext characters, satisfies both of the following two restrictions, where $\overline{\mathtt{m}}$ denotes the character immediately preceding $\mathtt{m}$ in M, then it is taken as $\sigma(\mathtt{m})$. Otherwise, Step 1 is restarted.[3]
   - 3.1. The first character of $\sigma(\mathtt{m})$ must never lie in the line used to encrypt $\overline{\mathtt{m}}$ (although it may be either colinear or non-colinear with the last character of $\sigma(\overline{\mathtt{m}})$).
   - 3.2. If $\xi_P(\overline{\mathtt{m}})$ = 1, 2, 4, 8, or 16 then the first character of $\sigma(\mathtt{m})$ must be non-colinear with the single character of $\sigma(\overline{\mathtt{m}})$ (which is a stronger requirement than 3.1).

Finally, the strings produced in Step 3 for each character of M are concatenated forming C.

As a result of the restrictions contained in Steps 1 and 3, the resulting ciphertext cryptogram C, consisting of the string $\sigma(\mathtt{m}_1)\sigma(\mathtt{m}_2)\sigma(\mathtt{m}_3)$... can be unambiguously

[2] Thus for each successive plaintext character the process alternates between reading rows left-to-right or right-to-left and between reading columns and diagonals top-down or bottom-up.

[3] It's fairly straightforward to show that some combination of choices made in Steps 1 and 3 satisfying all the restrictions must exist unless $\xi_P(\mathtt{m}) \times \xi_P(\overline{\mathtt{m}}) = 16$ for two consecutive plaintext characters, which would require the two consecutive ciphertext characters to lie in the same row. Accordingly, for each key there are five bigrams which cannot be encrypted by the algorithm. In the example above, they are `OE`, `NS`, `PP`, `SN`, and `EO`.

decrypted into the plaintext message $M = m_1m_2m_3$... by means of the decryption algorithm D defined as follows:

***Core cipher decryption algorithm:* M ⇐ D(K,C)**

> C is divided into contiguous groups of characters, proceeding from left to right, at each stage grouping as large an initial segment of the remaining ciphertext as possible composed of colinear characters of M_K, then inverting the association between binary numbers and subsets of column, row, or diagonal elements invoked in step 2 of the encryption algorithm, and finally decoding that number by inverting the substitution ξ_P.

Thus each plaintext character m is encrypted by randomly choosing a line of the key matrix M_K and representing that character's numerical code $\xi_P(m)$ by an n-tuple $\sigma(m)$ of characters lying in the chosen line. So that in decryption it will be possible to tell where one encrypted character ends and the next begins, $\sigma(m)$ is not allowed to begin with any character lying in the line chosen for $\sigma(\bar{m})$.

With any key, of the 31 characters comprising the plaintext alphabet A:
five are mapped by step 3 into one of 5 length-1 ciphertext unigrams,
ten are mapped by step 3 into one of 20 x 2! = 40 length-2 ciphertext bigrams,
ten are mapped by step 3 into one of 20 x 3! = 120 length-3 ciphertext trigrams,
five are mapped by step 3 into one of 20 x 4! = 480 length-4 ciphertext 4-grams, and
one is mapped by step 3 into one of 20 x 5! = 2400 length-5 ciphertext 5-grams,
resulting in a total of 3,045 possible cipher tokens.

3. Example encryption with the core cipher:

Continuing with the previous example key, the encryption process can be summarized as

A odd	13	01101	DCØ N2P	SV? SMY	ME- VE7	KRZ 1U8	Y7X ?-X	SEX YR?	MRØ D7-	K7? SCZ	YC- MVX	DVZ KEØ
A even	13	01101	4CO T2O	1VN KMD	UE2 REC	GRT GU4	87P Z-Ø	GEO URO	8RN G7N	472 8C2	1CT 4VT	UVP 1EP
B	31	11111	ODC4Ø ON2TP	NSV1? DSMKY	2MEU- CVER7	TKRGZ 41UG8	PY78X Ø?-ZX	OSEGX OYRU?	NMR8Ø ND7G-	2K74? 2SC8Z	TYC1- TMV4X	PDVUZ PKE1*
C	14	01110	DC4 N2T	SV1 SMK	MEU VER	KRG 1UG	Y78 ?-Z	SEG YRU	MR8 D7G	K74 SC8	YC1 MV4	DVU KE1
D odd	7	00111	C4Ø 2TP	V1? MKY	EU- ER7	RGZ UG8	78X -ZX	EGX RU?	R8Ø 7G-	74? C8Z	C1- V4X	VUZ E1Ø
D even	7	00111	ODC ON2	NSV DSM	2ME CVE	TKR 41U	PY7 Ø?-	OSE OYR	NMR ND7	2K7 2SC	TYC TMV	PDV PKE
E odd	16	10000	O	N	2	T	P					

E even	16	10000	Ø	?	-	Z	X					
F odd	5	00101	CØ 2P	V? MY	E- E7	RZ U8	7X -X	EX R?	RØ 7-	7? CZ	C- VX	VZ EØ
F even	5	00101	OC O2	NV DM	2E CE	TR 4U	P7 Ø-	OE OR	NR N7	27 2C	TC TV	PV PE

etc., where, in each row, the groups of characters comprising the rightmost ten columns are the subsets referred to in Step 2 of the encryption algorithm. In other words, A is randomly transformed into one of the six permutations of one of the twenty triples in either row 1 or row 2, depending on whether its location in M is odd or even; B is randomly transformed into one of the 120 permutations of one of the twenty quintuples in row 3; C is randomly transformed into one of the six permutations of one of the twenty triples in row 4; D is randomly transformed into one of the six permutations of one of the twenty triples in either row 5 or row 6, depending on whether its location in M is odd or even; E is randomly transformed into one of the five characters in either row 7 or row 8, depending on whether its location in M is odd or even; F is randomly transformed into one of the two permutations of one of the twenty doubles in either row 9 or row 10, depending on whether its location in M is odd or even; etc., subject to the restrictions specified in steps 1 and 3.

So, for example, the plaintext CATS AND DOGS can be encrypted as follows[4]:

m	$\xi_P(m)$		C/R/D	σ(m)	
C	14	01110	R_1	2NT	
A	13	01101	C_3	EU2	
T	3	00011	D_1	GX	
S	8	01000	C_2	1	
^	24	11000	R_2	DS	
A	13	01101	D_1	OGE	(O chosen to be colinear with preceding S)
N	2	00010	C_1	4	
D	7	00111	C_3	E2M	
^	24	11000	C_5	PY	
D	7	00111	D_{10}	KPE	(K chosen to be colinear with preceding Y)
O	1	00001	C_2	?	
G	22	10110	C_3	EM-	
S	8	01000	C_4	K	

yielding the ciphertext

2NTEU2GX1DSOGE4E2MPYKPE?EM-K

[4] In the middle column $\xi_P(m)$ is expressed in binary; in the fourth column the row, column, or diagonal chosen in Step 1 is indicated.

Note that Ø could not have been chosen instead of ? for σ(O) according to restriction 3.1. but - could have been, if a colinear character was called for. Similarly, neither -EM nor -ME could have been chosen instead of ME- for σ(G) according to restriction 3.2. Also note that R_2 could not have been used to encrypt G for then it would have been impossible to encrypt the following S. Except for the second A and the second D, non-colinearity was chosen instead of colinearity.

The ciphertext would be decrypted by dividing it, according to the table T_K, into its constituent k-tuples and then finding each group's associated binary number, converting to decimal, and decoding by inverting the substitution ξ_P

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$\xi_P^{-1}(n)$:	O	N	T	P	F	L	D	S	M	K	Y	,	A	C	V	E	R	W	I	H	U	G	.	^	?	-	Z	X	Q	J	B

For a slightly larger example consider the 230-character plaintext[5]

```
It haunts me, the passage of time. I think time is a merciless thing. I
think life is a process of burning oneself out and time is the fire that
burn-s you. But I think the spirit of man is a good adversary.  --
Tennessee Williams
```

which can be encrypted by the core cipher in (63 x 5) x (104 x 2 x 20) x (55 x 6 x 20) x (5 x 24 x 20) x (3 x 120 x 20) ≈ 1.5 x 10^{17} ways including, for example, this 471-character ciphertext:

```
ZØXSN DPR?E M-OXE 8DOM1 ?PNZ7 YZ8-G ØENUZ 7TO2D 1ZSCR KZPG8 -VP?Ø S21-T
DKNK? 72DO1 48ONØ ?MDØN MGY1M 2DP1Ø PCRNK YN8ØU SO78P MN24N XOUYR 814E1
XD8DN KTØ-S YD8?X -84UG 7RXØZ GX1?M Y1?NK UMXGR GOØD8 UØTM2 K?MZX CSZ1Ø
7OP?D 7GPGM ?1Ø7P Ø?EKP 1Ø2OP ?28TZ K8VDZ NMTUX K-RGP VOSP? VNTYD S4OCG
Y7PS2 YOZUP G4PG- ØZXUT YMTEC X14-Ø U2-O? T8XTP MY?RY 2S?ØK P1ØE? VNYD1
R7VYZ G81GP RNØ2M -E41O 4ØDCX 7PM2D NY-TD PCV27 OSX1M 4SNYT MDXDN 4E?SN
XOZDP 4?8GØ TCNO8 2XY7S Ø?2SZ YØ1ZD VGXRE CNZND 7SO1P EYKMN 8MR2X ØST1C
PO8S2 ØR8NU Z41ZD UN8MZ XR7Z1 D21D? P?4RC M2-8C KENG- TV4ZK 8
```

parsed as:

```
I   t  ^  h  a   u   n t  s ^  m  e ,  ^  t  h  e ^  p a   s s a   g   e
Z0X SN DP R? EM- OXE 8 DO M 1? PN Z 7Y Z8 -G 0E N UZ 7 TO2 D 1 ZSC RKZ P

^  o f  ^  t  i   m  e .    ^  I   ^  t  h  i   n k  ^  t  i   m  e ^
G8 - VP ?0 S2 1-T DK N K?72 DO 148 ON 0? MD 0NM G Y1 M2 DP 10P CR N KY

i   s ^  a   ^  m  e r  c   i   l  e s s ^  t  h  i   n g   .    ^  I
N8Ø U SO 78P MN 24 N XO UYR 814 E1 X D 8 DN KT Ø- SYD 8 ?X- 84UG 7R XØZ

^  t  h  i   n k  ^  l  i   f  e ^  i   s ^  a   ^  p r  o c   e s s ^
GX 1? MY 1?N K UM XG RG OØD 8U Ø TM 2K? M ZX CSZ 1Ø 7 OP ? D7G P G M ?1

o f  ^  b     u   r  n i   n g   ^  o n e s e l  f  ^  o u   t  ^  a   n
Ø 7P Ø? EKP1Ø 2OP ?2 8 TZK 8 VDZ NM T U X K - RG PV OS P ?VN TY DS 4OC G

d   ^  t  i   m  e ^  i   s ^  t  h  e ^  f  i   r  e ^  t  h  a   t  ^
Y7P S2 YO ZUP G4 P G- ØZX U TY MT EC X 14 -Ø U2- O? T 8X TP MY ?RY 2S ?Ø
```

---

[5] A dash is included in the plaintext word "burn-s" because this choice of key does not allow the bigram NS to be encrypted (see footnote 3).

```
b     u   r  n -   s ^  y   o u   .    ^  B     u   t  ^  I   ^  t  h
KP1ØE ?VN YD 1 R7V Y ZG 81G P RNØ 2M-E 41 O4ØDC X7P M2 DN Y-T DP CV 27

i   n k  ^  t  h  e ^  s p i   r  i   t  ^  o f  ^  m  a   n ^  i   s ^
OSX 1 M4 SN YT MD X DN 4 E ?SN XO ZDP 4? 8G Ø TC NO 82 XY7 S Ø? 2SZ Y Ø1

a   ^  g   o o d   ^  a   d   v    e r  s a   r  y   .    ^  ^  -   -
ZDV GX REC N Z ND7 SO 1PE YKM N8MR 2 XØ S T1C PO 8S2 ØR8N UZ 41 ZDU N8M

^  T  e n n e s s e e ^  W  i   l  l  i   a   m  s
ZX R7 Z 1 D 2 1 D ? P ?4 RC M2- 8C KE NG- TV4 ZK 8
```

4. Handycipher

Although the core cipher affords a reasonable level of security when used to encrypt relatively short plaintexts, with increasing message length it becomes more vulnerable to statistically based hill-climbing attacks along the lines described by Dhavare, et al [3]. Indeed, an earlier version of Handycipher was broken by just such an attack [1][2]. However, the cipher can be made significantly resistant to such attacks by the simple expedient of randomly dispersing so-called *null characters*, the fifteen characters comprising the last three columns of T_K, as decoys throughout the ciphertext. This is accomplished according to the following encryption algorithm $E^\dagger$ defined as follows:

***Handycipher encryption algorithm:* $C \Leftarrow E^\dagger(K,M)$**

This algorithm is identical to the core cipher encryption algorithm except that the final sentence

Finally, the strings produced in Step 3 for each character of M are concatenated forming C.

is replaced by the following text:

Finally, the strings produced in Step 3 for each character of M are concatenated forming C, and then null characters are inserted throughout C* in a statistically-balanced manner producing the cryptogram C by the following process:*

To create C, start with the stream of characters C.*

(1) With probability 5/8 insert the current character from C into C and repeat from (1) considering the next character in C*. If there is no next character, still repeat from (1) and stop only when there is a demand for a non-null (i.e. be prepared to insert more nulls).*

(2) Instead choose to insert a null into C. This null N, should be randomly chosen from the set of 15, but potentially rejected in favor of another null by considering the current last six characters of C. If N last appears at a position n characters back from the end of C, that N should be rejected with probability (6-n)/5. This leads to 100% rejection at n=1, i.e. consecutive identical characters are not allowed. Once a null is inserted, repeat (1) with the same current character in C as before, i.e. all characters in C* end up in C.*

This process should ensure that each individual character in C (null or non-null) is roughly equally common and that nulls are not betrayed by repeating too often within a few characters. Non-null characters are suppressed in their ability to repeat by the algorithm given the presence of the colinear groups, which can be as long as five characters. The likelihood of a null being the first, last, or any other character is constant.

The corresponding decryption is simply accomplished as:

Handycipher decryption algorithm: **M ⇐ D†(K,C)**

This algorithm is identical to the core cipher decryption algorithm except that the phrase

proceeding from left to right,

is amended to read:

proceeding from left to right and omitting null characters,

5. Example encryption with Handycipher

Continuing with the example in Section 3, encrypting the Tennessee Williams quotation with Handycipher instead of the core cipher might yield this 753-character ciphertext:

```
ZØXBS .IN26 S-7.M R6ØQW TZIR4 NB6OM 1W5?P NZLFY RXWZP T,FH8 UN5BZ XCN1H VYGQY
CJ-?B K7T?Q 1X2EQ DISTM 6DQKY 32UNX .6WTV MOQY5 2W?KN BO149 RNXØF ?8DUT MO6SW
8G4LN GP-6G C73R1 OASU. 2EW41 OI4P4 98EK1 2SFZ7 G9LFX K8BVQ CJOHS I34HU WKTJZ
1679Y X2TPO 89XQ- Q2UGA 8L?UX WQ-FR 5CIW. 37K5J VRXZQ 4V.2L M-P25 ZOJST KZMGJ
8EAL. FV71? EDYØ7 4KO1M Z8BAX N,VFO QDEIU M2-89 U4,PØ UW6IT Z3AKU S,ZCP AD,3,
O1BF5 ,XK9X C68VN A412R TBZIM 2DPH5 QRU,O B16WJ 2JM65 QES2Y 3OZ6X 5IØ24 L.PGZ
.1-T8 ?,ØLA HSO7J 2HØIY 9BLOV NZØ5X 2?QP- 1X4P2 8L16Q UND2S 9LTWY Q13CJ .,-27
I?TXU 5,7VR 9QK5H BXI8Q K6?L3 9HI4N ,ALFC EQ7D- 7NVCG KRQZA TE7CF ,PJKC VOXSB
ITKND .TRJS O5FXU HS86K QT,JS O72Ø. JLTY4 RJ2ZS ØPSFX OKYQ- 1XI2O 1W4PI 86EVQ
7SPB. QY419 8DQ8A G?F6. Y,LIR 36X4P 87A5O 9ZEJ3 FCV3M N7BNQ LW,HG CA91B -O4DC
P?H2Y QFZØA -T-HK 432WG ATRIZ 3L?12 MZDU9 WJØ?6 Z7,RX 4F-4A Y21DX .N5U? T59IL
45-3N ID5FR EY71T JFA6- 8PW.W AF.QJ 6W7K6 QØG
```

parsed as:

```
I   t     ^   h  a     u      n t    s ^    m  e ,    ^   t  h     e
ZØX BS.IN 26S -7 .MR6Ø QWTZIR 4 NB6O M 1W5? PN Z LFYR XWZ PT ,FH8U N

^    p a    s s a     g    e ^   o f  ^    t  i     m   e .       ^
5BZX C N1HV Y G QYCJ- ?BK7 T ?Q1 X 2E QDIS TM 6DQKY 32U N X.6WTVM OQY

I     ^   t  h   i    n k  ^  t   i    m   e ^   i    s ^   a    ^
52W?K NBO 14 9RN XØF? 8 DU TM O6S W8G4 LNG P -6G C73R 1 OAS U.2E W41

m   e r   c   i    l  e    s s ^    t    h     i     n g     .    ^
OI4 P 498 EK1 2SFZ 7G 9LFX K 8 BVQC JOHS I34HU WKTJZ 1 679YX 2TPO 89X

I     ^   t   h    i         n k    ^  l   i     f  e  ^   i   s ^
Q-Q2U GA8 L?U XWQ- FR5CIW.37 K 5JVR XZ Q4V .2LM- P2 5Z OJS TKZ M GJ8

a       ^  p r  o c   e s s ^  o   f   ^    b      u    r   n i
EAL.FV7 1? E DY Ø 74K O 1 M Z8 BAX N,V FOQD EIUM2- 89U4 ,PØ U W6ITZ3AK
```

```
n g    ^   o    n e     s e  l   f  ^   o u    t   ^  a       n
U S,ZC PAD ,3,O 1 BF5,X K 9X C68 VN A41 2 RTBZ IM2 DP H5QRU,O B1

d          ^  t   i      m  e   ^  i    s ^   t     h   e  ^      f
6WJ2JM65QE S2 Y3O Z6X5IØ 24 L.P GZ .1-T 8 ?,Ø LAHSO 7J2 HØ IY9BLO VN

i    r  e  ^  t  h  a      t  ^  b             u    r  n -     s
ZØ5X 2? QP -1 X4 P2 8L16QU ND 2S 9LTWYQ13CJ.,- 27I? TX U 5,7VR 9QK

^      y          o u        .    ^  B       u   t     ^  I   ^
5HBXI8 QK6?L39HI4 N ,ALFCEQ7 D-7N VC GKRQZAT E7C F,PJK CV OXS BITK

t  h   i      n k   ^    t    h  e ^     s p i    r  i    t  ^   o
ND .TR JSO5FX U HS8 6KQT ,JSO 72 Ø .JLTY 4 R J2ZS ØP SFXO KY Q-1 X

f   ^   m   a     n ^     i    s ^    a         ^    g   o   o
I2O 1W4 PI8 6EVQ7 S PB.QY 4198 D Q8AG ?F6.Y,LIR 36X4 P87 A5O 9Z

d      ^   a         d      v    e r   s a      r  y     .
EJ3FCV 3MN 7BNQLW,HG CA91B- O4DC P ?H2 Y QFZØA- T- HK432 WGATRIZ

^    ^  -   -       ^   T  e  n n  e s s e e  ^   W      i      l
3L?1 2M ZDU 9WJØ?6Z 7,R X4 F- 4 AY 2 1 D X .N 5U? T59IL4 5-3NID 5FRE

l  i       a             m    s
Y7 1TJFA6- 8PW.WAF.QJ6W7 K6QØ G
```

6. References

1. S. Combes, Handycipher decrypt (2014), available at http://oilulio.wordpress.com/2014/06/19/handycipher-decrypt/.
2. S. Combes, Breaking Handycipher 2 (2014), available at http://oilulio.wordpress.com/2014/07/28/breaking-handycipher-2/.
3. A. Dhavare, R. M. Low, M. Stamp, Efficient cryptanalysis of homophonic substitution ciphers, *Cryptologia* **37** (2013) 250-281.
4. B. Kallick, Handycipher: a Low-tech, randomized, symmetric-key cryptosystem, available at http://eprint.iacr.org/2014/257.pdf