Handycipher: a Low-tech, Randomized, Symmetric-key Cryptosystem

Bruce Kallick
Curmudgeon Associates
Winnetka, IL 60093
curmudgeon@rudegnu.com

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 using a nondeterministic encryption procedure, multiple encryption, and randomly generated session keys.

1. Introduction

For several thousand years cryptography was concerned largely with developing various kinds of substitution and transposition ciphers which, through sharing a manageably sized secret key, permitted easy encryption and decryption of messages using nothing more than pen and paper. This has all changed, of course, within our lifetime and now with public key cryptosystems, employing massively powerful computers, so-called hand ciphers are for the most part interesting only to historians and hobbyists.

Yet one can conceive of circumstances in which a highly secure pen-and-paper cipher would be invaluable; for example, someone needing to send or receive a secret message might not have access to a secure computer, or might need to refrain from using one to avoid arousing suspicion that messages are being exchanged secretly. Indeed, Bruce Schneier, a cryptographer and fellow at Harvard's Berkman Center, designed the Solitaire cipher [7] used in the novel *Cryptonomicon* for such a scenario.

Moreover, apart from any consideration of potential real-world applications, it is an interesting challenge to explore how much security against a large-scale computer-based cryptanalytic attack can be achieved using nothing more than a few hours of effort with pen and paper. The problem of designing such a cipher has received little attention in the recent cryptographic literature, and Schneier's Solitaire is widely regarded as the best serious attempt to deal effectively with this problem yet to have been devised. In this paper we describe a cipher which compares favorably in that it is somewhat easier to implement by hand, is less subject to error propagation, and needs no additional equipment besides pen and paper (unlike Solitaire which requires an ordered deck of cards).

In his seminal 1949 paper which heralded the emergence of modern cryptography, Shannon [8] observed:

> ...we can frame a test of ciphers which might be called the acid test. It applies only to ciphers with a small key (less than, say, 50 decimal digits), applied to natural languages, and not using the ideal method of gaining secrecy. The acid test is this: How difficult is it to determine the key or a part of the key knowing a small sample of message and corresponding cryptogram? [...] Note that the requirement of difficult solution under these conditions is not, by itself, contradictory to the requirements that enciphering and deciphering be simple processes.

In this spirit, then, the cipher described in this paper is proposed as a candidate for a modern formulation of Shannon's acid test. Using a 165-bit key (just small enough to fit Shannon's definition although larger than the Advanced Encryption Standard 128-bit minimum key size), Handycipher incorporates a nondeterministic encryption procedure along the lines described by Rivest and Sherman [6], and employs multiple encryption as suggested by Merkle and Hellman [5], as well as a randomly generated session key for each message. Combining a simple 31-character substitution cipher with a 3,045-token nondeterministic homophonic substitution cipher results in a novel system which, while quite easy to implement by hand, confers enough complexity to the relationship between ciphertext and plaintext and that between ciphertext and key to achieve a significant level of computational security against both statistical analysis and known-plaintext, chosen-plaintext, and chosen-ciphertext attack models.

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.

2. The core cipher

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 0-9.[1] Some permutation of the 41 characters of A* is chosen as the secret shared key K, say for example,

`Z D B 9 H A ? G V 8 1 J M T O U K - Y 5 0 Q 4 L ^ W F E R 6 I N . C , 7 2 X S 3 P`

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

[1] It's important, of course, to be able to distinguish the digits 0 and 1 from the letters O and I.

Z	D	B	9	H	A	?	G
V	8	1	J	M	T	O	U
K	-	Y	5	0	Q	4	L
W	F	E	R	6	I	N	.
C	,	7	2	X	S	3	P

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

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

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 , . -  ? ^
ξP(m):5 3 27 2 22 21 7 4 24 9 14 18 10 25 12 31 17 23 30 11 13 8 20 29 16 1 28 26 15 6 19
```

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 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 U occupying position 21 = 10101 is encrypted into one of the six permutations of one of the twenty 3-tuples

{ZKC D-, BY7 952 H0X ZBH V1M KY0 WE6 C7X ZYX D5C B0, 9K7 H-2 Z5, D07 BK2 9-X HYC}

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

{VW 8F 1E JR M6 D9 8J -5 FR ,2 8R 16 JW MF VE ME VR 86 1W JF}

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

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 following three restrictions, where $\hat{m}$ denotes the character immediately following m in M,
     $\xi_P(m) \neq 1, 2, 4, 8$, or 16
     $\xi_P(\hat{m}) \neq 2^{5-j}$, if the position of the character $\hat{m}$ in M is an odd number
     $\xi_P(\hat{m}) \neq 2^{j-1}$, if the position of the character $\hat{m}$ in M is an even number
     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. $\xi_P(m)$ is expressed as a five digit binary number, $b_1b_2b_3b_4b_5$, and if the position of the character m in 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 m in 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]

[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. 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 $\bar{m}$ denotes the character immediately preceding m in M, then it is taken as σ(m). Otherwise, Step 1 is restarted.[3]

   3.1. The first character of σ(m) must never lie in the line used to encrypt $\bar{m}$ (although it may be either colinear or non-colinear with the last character of $\sigma(\bar{m})$).

   3.2. If $\xi_P(\bar{m})$ = 1, 2, 4, 8, or 16 then the first character of σ(m) must be non-colinear with the single character of $\sigma(\bar{m})$ (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 $\sigma(m_1)\sigma(m_2)\sigma(m_3)$... can be unambiguously 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 ξ_P(m) by an n-tuple σ(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, σ(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] It's fairly straightforward to show that some combination of choices made in Steps 1 and 3 satisfying all the restrictions must exist unless $\xi_P(m) \times \xi_P(\bar{m}) = 16$ 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. (See Appendix 1.)

3. Example encryption with the core cipher

Although any permutation of the entire ciphertext alphabet can be chosen as K, the problem of remembering and secretly sharing it can be made easier by formalizing a way of generating the key from a more memorable key passphrase. The following method is designed to work well with Handycipher. The passphrase is processed from left to right, first replacing all spaces by the number of characters in the preceding word, and then (again proceeding from left to right) omitting all repetitions; then ^ and all other characters missing from the resulting string are appended in reverse order, i.e., in the order:

{9–0 ^ ? - . , Z Y X W V U T S R Q P O N M L K J I H G F E D C B A}

A passphrase can be more easily communicated secretly than the key, for example by using, on the nth day of the year, the first fifty characters on the nth page of a previously agreed upon book. As a more fanciful example, the passphrase could be the first verse of a folk song, as in:

ON TOP OF OLD SMOKY, ALL COVERED WITH SNOW, I LOST MY TRUE LOVER FOR COURTING TOO SLOW.

which generates the key 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 0 ^ ? - Z X Q J B

and plaintext subkey P

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 associated table T_K

0	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
0	?	-	Z	X	Q	J	B

The substitution ξ_P can be written

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

and the encryption process can be summarized as

A odd	13	01101	DC0 N2P	SV? SMY	ME- VE7	KRZ 1U8	Y7X ?-X	SEX YR?	MR0 D7-	K7? SCZ	YC- MVX	DVZ KE0
A even	13	01101	4CO T2O	1VN KMD	UE2 REC	GRT GU4	87P Z-0	GEO URO	8RN G7N	472 8C2	1CT 4VT	UVP 1EP
B	31	11111	ODC40 ON2TP	NSV1? DSMKY	2MEU- CVER7	TKRGZ 41UG8	PY78X 0?-ZX	OSEGX OYRU?	NMR80 ND7G-	2K74? 2SC8Z	TYC1- TMV4X	PDVUZ PKE10
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	C40 2TP	V1? MKY	EU- ER7	RGZ UG8	78X -ZX	EGX RU?	R80 7G-	74? C8Z	C1- V4X	VUZ E10
D even	7	00111	ODC ON2	NSV DSM	2ME CVE	TKR 41U	PY7 0?-	OSE OYR	NMR ND7	2K7 2SC	TYC TMV	PDV PKE
E odd	16	10000	O	N	2	T	P					
E even	16	10000	0	?	-	Z	X					
F odd	5	00101	C0 2P	V? MY	E- E7	RZ U8	7X -X	EX R?	R0 7-	7? CZ	C- VX	VZ E0
F even	5	00101	OC O2	NV DM	2E CE	TR 4U	P7 0-	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]:

[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.

m	ξ_P(m)		C/R/D	σ(m)	
C	14	01110	R1	2NT	
A	13	01101	C3	EU2	
T	3	00011	D1	GX	
S	8	01000	C2	1	
^	24	11000	R2	DS	
A	13	01101	D1	OGE	(O chosen to be colinear with preceding S)
N	2	00010	C1	4	
D	7	00111	C3	E2M	
^	24	11000	C5	PY	
D	7	00111	D10	KPE	(K chosen to be colinear with preceding Y)
O	1	00001	C2	?	
G	22	10110	C3	EM-	
S	8	01000	C4	K	

yielding the ciphertext

`2NTEU2GX1DSOGE4E2MPYKPE?EM-K`

Note that `0` 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
ξ_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:

```
Z0XSN DPR?E M-OXE 8DOM1 ?PNZ7 YZ8-G 0ENUZ 7TO2D 1ZSCR KZPG8 -VP?0 S21-T
DKNK? 72DO1 48ON0 ?MD0N MGY1M 2DP10 PCRNK YN80U SO78P MN24N XOUYR 814E1
XD8DN KT0-S YD8?X -84UG 7RX0Z GX1?M Y1?NK UMXGR GO0D8 U0TM2 K?MZX CSZ10
```

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).

```
7OP?D 7GPGM ?107P 0?EKP 102OP ?28TZ K8VDZ NMTUX K-RGP VOSP? VNTYD S4OCG
Y7PS2 YOZUP G4PG- 0ZXUT YMTEC X14-0 U2-O? T8XTP MY?RY 2S?0K P10E? VNYD1
R7VYZ G81GP RN02M -E41O 40DCX 7PM2D NY-TD PCV27 OSX1M 4SNYT MDXDN 4E?SN
XOZDP 4?8G0 TCNO8 2XY7S 0?2SZ Y01ZD VGXRE CNZND 7SO1P EYKMN 8MR2X 0ST1C
PO8S2 0R8NU 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
N80 U SO 78P MN 24 N XO UYR 814 E1 X D 8 DN KT 0- SYD 8 ?X- 84UG 7R X0Z

^  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 O0D 8U 0 TM 2K? M ZX CSZ 10 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
0 7P 0? EKP10 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- 0ZX U TY MT EC X 14 -0 U2- O? T 8X TP MY ?RY 2S ?0

b     u   r  n -   s ^  y   o u   .    ^  B     u   t  ^  I   ^  t  h
KP10E ?VN YD 1 R7V Y ZG 81G P RN0 2M-E 41 O40DC 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 0 TC NO 82 XY7 S 0? 2SZ Y 01

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 X0 S T1C PO 8S2 0R8N 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
```

Although the average bandwidth expansion factor averaged over all possible keys and all possible messages uniformly distributed, is

$$(5 \times 1 + 10 \times 2 + 10 \times 3 + 5 \times 4 + 1 \times 5) / 31 \approx 2.58$$

for the example key above, noting the distribution of length-n expansions among the characters of A, namely

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

and using the usual frequency distribution of these 31 characters in English, an average bandwidth expansion factor can be computed as:

$$1 \times 0.28 + 2 \times 0.45 + 3 \times 0.23 + 4 \times 0.02 + 5 \times 0.01 \approx 2.2$$

while that of this particular encryption is $470 / 230 \approx 2.0$.

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 ⇐ E†(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:

```
Z0XBS .IN26 S-7.M R60QW TZIR4 NB6OM 1W5?P NZLFY RXWZP T,FH8 UN5BZ XCN1H VYGQY
CJ-?B K7T?Q 1X2EQ DISTM 6DQKY 32UNX .6WTV MOQY5 2W?KN BO149 RNX0F ?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? EDY07 4KO1M Z8BAX N,VFO QDEIU M2-89 U4,P0 UW6IT Z3AKU S,ZCP AD,3,
O1BF5 ,XK9X C68VN A412R TBZIM 2DPH5 QRU,O B16WJ 2JM65 QES2Y 3OZ6X 5I024 L.PGZ
.1-T8 ?,0LA HSO7J 2H0IY 9BLOV NZ05X 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 O720. JLTY4 RJ2ZS 0PSFX OKYQ- 1XI2O 1W4PI 86EVQ
7SPB. QY419 8DQ8A G?F6. Y,LIR 36X4P 87A5O 9ZEJ3 FCV3M N7BNQ LW,HG CA91B -O4DC
P?H2Y QFZ0A -T-HK 432WG ATRIZ 3L?12 MZDU9 WJ0?6 Z7,RX 4F-4A Y21DX .N5U? T59IL
45-3N ID5FR EY71T JFA6- 8PW.W AF.QJ 6W7K6 Q0G
```

parsed as:

```
I   t     ^   h  a     u      n t    s ^    m  e ,    ^   t  h     e
Z0X BS.IN 26S -7 .MR60 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 X0F? 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 0 74K O 1 M Z8 BAX N,V FOQD EIUM2- 89U4 ,P0 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 Z6X5I0 24 L.P GZ .1-T 8 ?,0 LAHSO 7J2 H0 IY9BLO VN

i    r  e  ^  t  h  a      t  ^  b             u    r  n -     s
Z05X 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 0 .JLTY 4 R J2ZS 0P 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 QFZ0A- T- HK432 WGATRIZ

^    ^  -   -       ^   T  e  n n  e s s e e  ^   W      i      l
3L?1 2M ZDU 9WJ0?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 K6Q0 G
```

6. Extended Handycipher

Extended Handycipher operates with the same plaintext and ciphertext alphabets, and encrypts a message M using a key K by first generating a random session key K′ and encrypting M with Handycipher using K′ to produce an intermediate ciphertext C′. K′ is then encrypted with Handycipher using K and embedded in C′ at a location based on K and the length of M, producing the final ciphertext C.

Extending Handycipher in this way confers several advantages in security at little computational cost. Because each plaintext message is encrypted with a different randomly generated session key, the primary secret key is less exposed to any attack that depends on having a lot of ciphertext to work with, and the security of the cipher is less compromised by encrypting multiple messages with the same key.

Extended Handycipher encryption algorithm: **C ⇐ E*(K,M)**

1. Generate a random 41-character key K′ with associated table T_K' and coding substitution ξ_P'.
2. Transcribe K′ into plaintext characters by spelling the ten digits and the word “space” and enclose each spelled word in a pair of spaces.
3. Encrypt the transcribed K′ with Handycipher and K, yielding K′′. Adjust K′′ if necessary ensuring that for the last character `m` of the transcribed K′ to be encrypted, no null characters are interspersed with σ(`m`) and that K′′ terminate with exactly one null character.[6]
4. Encrypt M with Handycipher and K′, yielding C′.
5. Adjust C′ if necessary, by inserting more nulls, ensuring that $|C'| + |K''| \geq 500$ and also that $N \geq 30 - R$ where $|C'| = 31 \cdot N + R,\ 0 \leq R < 31$.
6. Calculate j = $\lfloor(|C'| + |K''| - 500) / 31\rfloor \cdot \{[\xi_P(\text{A}) + \xi_P(\text{B}) + \xi_P(\text{C})] \bmod 31\} + [\xi_P(\text{D}) + \xi_P(\text{E}) + \xi_P(\text{F})] \bmod 31$.[7]
7. Insert K′′ into C′ immediately following position j as calculated in step 6, yielding C.

---

[6] This is necessary so that in Step 3 of the decryption algorithm the end of K′′ can be recognized.

[7] Here ⌊x⌋ denotes the integer part of x and |C| denotes the length of C. The formula is designed merely to make the value of j depend on K (and its subkey P) and |C|. The adjustments in Step 5 ensure that j ≤ |C|. (See Appendix 2.)

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

1. Calculate j =
   $\lfloor (|C| - 500) / 31 \rfloor \cdot \{[\xi_P(\text{A}) + \xi_P(\text{B}) + \xi_P(\text{C})] \bmod 31\} + [\xi_P(\text{D}) + \xi_P(\text{E}) + \xi_P(\text{F})] \bmod 31$
   and begin decrypting the substring of C immediately following position j with Handycipher and K.
2. Transcribe the spelled digits and the word “space” back into their ciphertext character equivalents.
3. Continue until 41 such characters have been decrypted, yielding the session key, K′.
4. Remove the decrypted substring from C, leaving C′.
5. Decrypt C′ with Handycipher and K′, yielding M.

7. Example encryption with Extended Handycipher

Continuing with the previous example, to encrypt the Williams quote with Extended Handycipher, at first a random 41-character session key K′ is generated, say the one used as an example in Section 2:

```
Z D B 9 H A ? G V 8 1 J M T O U K - Y 5 0 Q 4 L ^ W F E R 6 I N . C , 7 2 X S 3 P
```

with subkey P′

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

and associated table $T_{K'}$

Z	D	B	9	H	A	?	G
V	8	1	J	M	T	O	U
K	-	Y	5	0	Q	4	L
W	F	E	R	6	I	N	.
C	,	7	2	X	S	3	P

and coding substitution $\xi_{P'}$

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	,	.	-	?	^
$\xi_{P'}$(m):	5	3	27	2	22	21	7	4	24	9	14	18	10	25	12	31	17	23	30	11	13	8	20	29	16	1	28	26	15	6	19

The quote[8] is then encrypted with Handycipher using this $\xi_{P'}$ and $T_{K'}$, yielding, for example, this 1041-character ciphertext as C′

[8] A dash is included in the plaintext word “ad-versary” because this choice of key does not allow the bigram DV to be encrypted (see footnote 3).

```
,CQ8B I46GJ MUVAY 25WRE .DOCQ 1K-S5 4HV-G EX,P. C-5O8 LTM1K ?B8.9 UGP1X 4MJ85
HYFP1 DC9SP XTI-W N15ZR TFSWE XA-WS 1,5AI .QD51 0R3D, ATZM4 Y8,AZ 57DUR OBQWJ
DPZRJ G6H0S FN?7N MIOD7 3RF,4 SMVJW FRTKE ,A17B 5INM. ?LE7F 9EIB1 ZMQR. ?8HIF
3YTSG 6?WPF 1BX40 M67UR DEPW. IHX6S 38LR- UN9W3 M.,N5 Z1E7N BPN,S .GWRU WY?CQ
JK8B6 YO1U7 EKP50 OZ9IA DPK,E 1OADC 9MK.H 6MP2O HV,3C ?8VM6 82NY4 VHKL5 0156P
J2U9E GZQN0 57XCQ EFU6Z WNCR6 AUV1J 89?7U MCPY6 WTF0? P.TDO NRVT. 7-YK0 41Y3P
.OS6U PFR?W 5GR98 62KE. WFRHI CJ-PQ 1ZNKC T4E7B M98UT GLXY9 M7K1B PG7WX ?L71B
J95AU ?HCSF 4QS1J -.U0? KD4HU BOM9T KIFQ5 SMA,C L2.YQ STZX5 I0KPG E?LYT ,7XNV
IJ82S ACLNX UK98B 2M4I2 6B?.Q RAS8Z -KLEV SFHYL 92JZ? T80.? AY-5X W.938 ZO?R4
K.JS2 5HOX6 3G7X. CNMTO Z7,PX I?NC0 6H7DV F6ARK SXYGT 9RJ6X A4QHV HKSML 7I8UT
PSKB2 3WFN6 YEOG7 1,?.I ZTG4E UXDB- GF.DM ZUECX ,R420 RUNDQ X.2,1 .9XTJ B?8MU
VA,3. JSWUI 4YSV. 8TI?W RL6IB D9V.Z CMFN4 G7-.? B9AQZ 24HUT V95RJ ZKPSV WCB1Z
Y8XV3 ?U.8F HJ7BS EU?IW S3.Q0 ZPO,5 48,UD AP9GT DQWEK 0-CHJ K-MLT 6P0XC 4LUZW
-4DWO RP67L ,CMKJ 16VZC 04,LQ 1O3,M E5WHQ FUYN? .VQKN 3LZIO ?C9?P NFG?O MKN1V
B624T K,ITR O.4J9 ,ZOIM 6QHXB 0WJRA V0AQ7 S8B2W 1IXO3 BHQ?D XNLHM .KOU? U05N6
BGUON KRXGY I4T8H V-E8O P?KS2 FA9KS GQXZ8 CUIO7 UAE7Q 6H.8M TD3VP BO0F3 8E2VG
-
```

parsed as:

```
I  t      ^     h  a  u   n      t    s      ^     m  e      ,
,C Q8BI46 GJMUV AY 25 WRE .DOCQ1 K-S5 4HV-GE X,P.C -5 O8LTM1 K?B8

^       t    h e   ^    p          a  s      s      a  g       e
.9UGP1X 4MJ8 5 HYF P1DC 9SPXTI-WN1 5Z RTFSWE XA-WS1 ,5 AI.QD51 0R3D

^     o   f    ^    t      i   m  e    .       ^      I  ^      t   h  i
,ATZM 4Y8 ,AZ5 7DUR OBQWJ DPZ RJ G6H0 SFN?7NM IOD73R F, 4SMVJ WFR TK E,

n    k        ^   t    i  m     e     ^        i  s      ^    a   ^
A17B 5INM.?LE 7F9 EIB1 ZM QR.?8 HIF3Y TSG6?WPF 1B X40M6 7URD EPW .IHX6

m     e     r       c     i       l   e     s    s      ^    t      h
S38LR -UN9W 3M.,N5Z 1E7NB PN,S.GW RUW Y?CQJ K8B6 YO1U7E KP50 OZ9IAD PK

i  n     g   .    ^     I   ^    t   h  i   n    k   ^     l   i    f
,E 1OADC 9MK .H6M P2OHV ,3C ?8VM 682 NY 4VH KL50 156 PJ2U9 EGZ QN05 7XC

e     ^    i  s      ^     a   ^    p             r    o   c
QEFU6 ZWNC R6 AUV1J8 9?7UM CPY 6WTF 0?P.TDONRVT.7 -YK0 41Y 3P.OS6UPFR?W

e    s    s     ^    o    f    ^     b  u       r    n     i  n     g
5GR9 862K E.WFR HICJ -PQ1 ZNKC T4E7B M9 8UTGLXY 9M7K 1BPG7 WX ?L71B J95

^       o     n      e     s       e      l   f       ^    o      u
AU?HCSF 4QS1J -.U0?K D4HUB OM9TKIF Q5SMA, CL2 .YQSTZX 5I0K PGE?LY T,7X

t     ^       a   n   d ^     t        i  m   e    ^    i    s
NVIJ8 2SACLNX UK9 8B2 M 4I26B ?.QRAS8Z -K LEV SFHY L92J Z?T8 0.?AY-5

^    t      h  e     ^    f      i     r        e   ^   t    h a
XW.9 38ZO?R 4K .JS25 HOX6 3G7X.C NMTOZ 7,PXI?NC 06H 7DV F6AR K SXY

t     ^      b  u     r         n     s      ^         y  o  u     .
GT9RJ 6XA4QH VH KSML7 I8UTPSKB2 3WFN6 YEOG71 ,?.IZTG4E UX DB -GF.D MZUE
```

```
^   B   u     t     ^    I   ^     t       h    i    n       k    ^
CX, R42 0RUND QX.2, 1.9X TJB ?8MUV A,3.JSW UI4Y SV.8 TI?WRL6 IBD9 V.ZC

t      h e       ^      s    p       i  r    i      t   ^    o
MFN4G7 - .?B9AQZ 24HUTV 95RJ ZKPSVWC B1 ZY8X V3?U.8 FHJ 7BSE U?IWS3.Q0

f     ^     m      a   n   ^   i  s       ^      a   ^     g    o  o  d
ZPO,5 48,UD AP9GTD QWE K0- CHJ K- MLT6P0X C4LUZW -4D WORP6 7L,C MK J1 6

^   a   d   -      v e     r              s          a   r      y
VZC 04, LQ1 O3,ME5 W HQFUY N?.VQKN3LZIO?C 9?PNFG?OMK N1V B624TK ,

.        ^     ^    -    -       ^    T    e       n     n
ITRO.4J9 ,ZOIM 6QHX B0WJ RAV0AQ7 S8B2 W1IX O3BHQ?D XNLHM .KOU?U05

e        s        s    e       e    ^      W     i    l   l   i    a
N6BGUONK RXGYI4T8 HV-E 8OP?KS2 FA9K SGQXZ8 CUIO7 UAE7 Q6H .8M TD3V PBO0

m   s
F38 E2VG-
```

K′ is transcribed into plaintext characters as

ZDB nine HA?GV eight one JMTOUK-Y five zero Q four L space WFER six IN.C, seven two XS three P

and then encrypted with Handycipher and K yielding K″, for example,

```
?X0ZW QYC5T LS8JZ C2316 0HG0. MN5UI XKQPC JZVS5 ?9CRL 7OT5, A24LF MTBV2 KXA23
QU,HI -SZ.J CN7OH FYNSP T?MWJ P459? T1.YC UP?9F ,4NE6 C71GN 8W9MG 6BSO1 4P37,
U2-5Q 4.UG1 OZ.WG HLC9V G5W81 4T?W9 N5X1- NVS?G .5-VX BA.NH 5X0-6 48HBD PMEYP
H34RP WE1BM EU50A YTSY- 70BF5 TZ10S T-YJ. NH52O HL8ZG N-QJY I48HG UW,SF MKJVS
PTS0V BX49M QZQ1X A8TFK HNBMO G2VBC UVIFZ .Y5ZA XF9U6 B?.QE 7W9I5 LZ3T. 02LX4
E
```

The position at which the encrypted session key will be inserted is calculated as

$$j = \lfloor (|C'| + |K''| - 500) / 31 \rfloor \cdot \{[\xi_P(\mathrm{A}) + \xi_P(\mathrm{B}) + \xi_P(\mathrm{C})] \bmod 31\} + [\xi_P(\mathrm{D}) + \xi_P(\mathrm{E}) + \xi_P(\mathrm{F})] \bmod 31$$

$$= \lfloor (1041 + 326 - 500) / 31 \rfloor \cdot \{[13 + 31 + 14] \bmod 31\} + [7 + 16 + 5] \bmod 31$$

$$= 27 \cdot 27 + 28$$

$$= 757$$

K″ is inserted following the 757th character of C′, yielding C

```
,CQ8B I46GJ MUVAY 25WRE .DOCQ 1K-S5 4HV-G EX,P. C-5O8 LTM1K ?B8.9 UGP1X
4MJ85 HYFP1 DC9SP XTI-W N15ZR TFSWE XA-WS 1,5AI .QD51 0R3D, ATZM4 Y8,AZ
57DUR OBQWJ DPZRJ G6H0S FN?7N MIOD7 3RF,4 SMVJW FRTKE ,A17B 5INM. ?LE7F
9EIB1 ZMQR. ?8HIF 3YTSG 6?WPF 1BX40 M67UR DEPW. IHX6S 38LR- UN9W3 M.,N5
Z1E7N BPN,S .GWRU WY?CQ JK8B6 YO1U7 EKP50 OZ9IA DPK,E 1OADC 9MK.H 6MP2O
HV,3C ?8VM6 82NY4 VHKL5 0156P J2U9E GZQN0 57XCQ EFU6Z WNCR6 AUV1J 89?7U
MCPY6 WTF0? P.TDO NRVT. 7-YK0 41Y3P .OS6U PFR?W 5GR98 62KE. WFRHI CJ-PQ
1ZNKC T4E7B M98UT GLXY9 M7K1B PG7WX ?L71B J95AU ?HCSF 4QS1J -.U0? KD4HU
BOM9T KIFQ5 SMA,C L2.YQ STZX5 I0KPG E?LYT ,7XNV IJ82S ACLNX UK98B 2M4I2
```

```
6B?.Q RAS8Z -KLEV SFHYL 92JZ? T80.? AY-5X W.938 ZO?R4 K.JS2 5HOX6 3G7X.
CNMTO Z7,PX I?NC0 6H7DV F6ARK SXYGT 9RJ6X A4QHV HKSML 7I8UT PSKB2 3WFN6
YEOG7 1,?.I ZTG4E UXDB- GF.DM ZUECX ,R420 RUNDQ X.2,1 .9XTJ B?8MU VA,3.
JSWUI 4YSV. 8TI?W RL6IB D9V.Z CMFN4 G7-.? B9?X0 ZWQYC 5TLS8 JZC23 160HG
0.MN5 UIXKQ PCJZV S5?9C RL7OT 5,A24 LFMTB V2KXA 23QU, HI-SZ .JCN7 OHFYN
SPT?M WJP45 9?T1. YCUP? 9F,4N E6C71 GN8W9 MG6BS O14P3 7,U2- 5Q4.U G1OZ.
WGHLC 9VG5W 814T? W9N5X 1-NVS ?G.5- VXBA. NH5X0 -648H BDPME YPH34 RPWE1
BMEU5 0AYTS Y-70B F5TZ1 0ST-Y J.NH5 2OHL8 ZGN-Q JYI48 HGUW, SFMKJ VSPTS
0VBX4 9MQZQ 1XA8T FKHNB MOG2V BCUVI FZ.Y5 ZAXF9 U6B?. QE7W9 I5LZ3 T.02L
X4EAQ Z24HU TV95R JZKPS VWCB1 ZY8XV 3?U.8 FHJ7B SEU?I WS3.Q 0ZPO, 548,U
DAP9G TDQWE K0-CH JK-ML T6P0X C4LUZ W-4DW ORP67 L,CMK J16VZ C04,L Q1O3,
ME5WH QFUYN ?.VQK N3LZI O?C9? PNFG? OMKN1 VB624 TK,IT RO.4J 9,ZOI M6QHX
B0WJR AV0AQ 7S8B2 W1IXO 3BHQ? DXNLH M.KOU ?U05N 6BGUO NKRXG YI4T8 HV-E8
OP?KS 2FA9K SGQXZ 8CUIO 7UAE7 Q6H.8 MTD3V PBO0F 38E2V G-
```

8. Cryptanalytic vulnerability

Although the original version of Handycipher was fairly secure for a pen-and-paper cipher in encrypting short (say, less than 200-character) messages, for longer ones it proved to be vulnerable to statistically based hill-climbing attacks similar to those described in Dhavare, et al. [3]. After the original cipher was broken by such a method [1] a subsequent version attempted to repair its vulnerability with an elaborate scheme using strings of null characters as escape markers followed by decoy strings of non-colinear characters but that version, like the previous one, fell victim to the discoverability of the five null characters [2].

This version of the cipher has been made highly resistant to such attacks by adding ten characters to the ciphertext alphabet, using a 41-character key instead of 31, increasing the number of null characters from five to fifteen, increasing the number of diagonals used from two to ten, and alternating the direction of encoding plaintext characters between top-down/left-right and bottom-up/right-left.

The way that the random choices are made in Steps 1 and 3 of the core cipher encryption algorithm, and also in the null character insertion process of the Handycipher encryption algorithm, will have a significant effect on the cipher's vulnerability to statistically based attacks. In Step 1, the choices of R_1–R_5, C_1–C_5, and D_1–D_{10} should all be equally probable, and in Step 3, each permutation of the string $\sigma(m)$ should be equally probable. This can be accomplished with the use of a single six-sided die (as described, for example, by Reinhold [4]) or one can improve one's skill at behaving randomly by visiting Chris Wetzel's website [9]. For very short messages, it might be sufficient for these choices merely to be made nondeterministically, but as message length increases any departure from choosing randomly is likely to compromise the cipher's security against statistically based attacks.

The sole purpose of randomly inserting null characters into the ciphertext is to defeat hill-climbing attacks against the undisguised ciphertext produced by the core encryption algorithm. Although it might be sufficient for shorter messages merely to insert null characters nondeterministically, as message length increases it becomes more important that they be inserted in the statistically balanced way described in the encryption algorithm to avoid their being detectable by statistical analysis.

Similarly, for longer messages (say, more than 600 characters) a significant strengthening of the core cipher against statistically based attacks can be achieved by making the random choices in Steps 1 and 3 in a statistically balanced way rather than purely at random. It turns out that not only is it always possible to choose $\sigma(\mathtt{m})$ in Step 3 satisfying all the restrictions, it is additionally always possible to choose whether the first character of $\sigma(\mathtt{m})$ is colinear or non-colinear with the last character of $\sigma(\overline{\mathtt{m}})$ unless restriction 3.2 requires it to be non-colinear.[9] If this choice between colinearity and non-colinearity is made purely randomly, it opens a vulnerability to a hill-climbing attack based on a metric measuring the percentage of all consecutive characters in a target ciphertext which are colinear with respect to each possible key-matrix. It can be shown that with respect to a randomly chosen key-matrix the expected value of this metric applied to a Handycipher generated cryptogram is 2/3, whereas with respect to the correct key-matrix the value will tend to be higher (because each $\sigma(\mathtt{m})$ comprises a group of colinear characters) and this difference can be exploited by a hill-climbing attack. Increasing the probability of choosing non-colinearity in Step 3 decreases the colinearity metric and it has been determined empirically that the value approaches 2/3 as the probability of choosing non-colinearity over colinearity in Step 3 approaches 7/8.

In previous versions of the cipher with only five null characters and a 30-character key table, an attack could be mounted by examining all 142,506 possible null character set choices as was done in [1]; with fifteen nulls out of 40 and 40,225,345,056 possible choices such an attack is very hard. Moreover, unlike previous versions, even discovering the set of nulls would give no information about where the divisions occur in the ciphertext and when removed the remaining ciphertext would still remain quite secure as argued in the last paragraph..

The alternating reversal of coding direction may only be necessary for longer messages and could be improved by building into the key an indication of some other arbitrary pattern of alternation to be followed—for example, the choice of null character used to mark the end of the embedded session key in Extended Handycipher could be so used. However, the most secure way of encrypting very long messages would seem to be to divide them into shorter ones and encrypt each using Extended Handycipher ensuring that none of the randomly generated session keys will be as exposed by a very long plaintext.

Another vulnerability presented by encrypting very long plaintexts is that the nulls, which are distributed by the cipher evenly in terms of aggregate numbers, will likely be distinguishable by tending towards their expected frequency value while the non-nulls will diverge from the expected value to a statistically significant degree.

---

[9] This is a bit trickier to prove, but essentially it just requires adding an additional restriction requiring that whenever $\xi_P(\hat{\mathtt{m}})$ is a power of 2, the last character of $\sigma(\mathtt{m})$) not lie in the row which must contain $\sigma(\hat{\mathtt{m}})$, where $\hat{\mathtt{m}}$ denotes the character immediately following m in M

With respect to known-plaintext and chosen-plaintext resistance, the homophonic nature of the cipher (using 3,045 possible homophonic tokens for the core cipher and an unbounded number when nulls are employed), together with the fact that each token is composed of a variable length string of symbols, is a very strong counter to such attacks. In effect an attacker must try all possible symbol lengths to try to synchronize with the text he knows. Also, the use of session keys would further limit the benefits of chosen or known-plaintext as such text only betrays itself. Similarly, the risk of the same message being encrypted twice with different keys is reduced.

The cipher would clearly be vulnerable to a chosen text of long repetitions of characters (e.g. the five singletons would ultimately reveal the five rows of the session-key matrix) but it seems unlikely a hand cipher user would be trapped in this way. However it does imply that Handycipher would be a poor choice to implement in a micro controller with a fixed key.

9. Challenge cryptograms

Two 700-character plaintext messages M_1 and M_2 have each been encrypted with Extended Handycipher using the same key K, yielding the two cryptograms C_1 and C_2 contained in Appendix 3, not necessarily in that order. The first 229 characters of M_1 consist of the Williams quotation in Section 3 (without the inserted dash in the word "burns"). Four challenges in increasing order of difficulty are offered:

1. Determine whether C_1 is the encryption of M_1 or of M_2.
2. Reveal the plaintext following the first 229 characters of M_1.
3. Reveal M_2.
4. Reveal K.

10. Implementation notes

10.1. Although the process is tedious, with a bit of practice one can reasonably expect to encrypt or decrypt messages with Handycipher at a rate of approximately three plaintext characters per minute. At that rate the 229 character Williams quotation takes about an hour and a quarter to encrypt and perhaps an additional 30 minutes to generate, encrypt, and insert a session key.

10.2. In order to facilitate visualizing the extended diagonals it may be helpful to think of the matrix as a 5 x 5 chess board (where the rows, columns, and diagonals wrap around the edges) and recognize that for any given square there are 16 other colinear squares and eight non-colinear squares—those that are a knight's move away.

10.3. Although there is little propagation of errors in both encrypting and decrypting (except for possibly disturbing synchrony as discussed in 10.4 below) special care should be taken when processing the session key K′ since any error introduced into a key obviously will be propagated.

10.4. If an error is made in keeping track of the alternating direction of encrypting plaintext characters or decrypting groups of ciphertext characters (or if some other error causes such a disruption), the receiver will immediately notice what has happened and can adjust to keep in synchrony. (It might even be a useful ploy to do this intensionally several times to thwart some types of attack.)

10.5. Null characters should certainly be introduced in encrypting the session key so that its length is not predictable, and the encryption of the 41st session key character must contain only a single null character at its end to ensure that its boundary is demarcated in the decryption process.

10.6. Frequency distribution of ciphertext characters can be further flattened by modifying K′, in Step 1 of the Extended Handycipher encryption algorithm, so that the most common plaintext letters will not be encrypted by K′ into unigrams.

10.7. Similarly, to avoid having to insert many dashes into the plaintext, K′ can be modified so that no very common plaintext bigram is among the five that cannot be encrypted by K′.

10.8. Before proceeding to Step 3 of the Extended Handycipher encryption algorithm, K′ should also be modified, if necessary, so that the transcribed K′ generated in Step 2 contains none of the five plaintext bigrams that cannot be encrypted by K.

10.9. Source code for a full Python implementation of Handycipher and Extended Handycipher, as well as several additional Handycipher-based challenges, are available at: <https://www.mysterytwisterc3.org/>.

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. R. Merkle, M. Hellman, On the security of multiple encryption, *CACM* **24** (1981) 465-467.

5. A. G. Reinhold, How do I use dice to create random character strings?(1995), available at http://world.std.com/%7Ereinhold/dicewarefaq.html#randomstrings.

6. R. L. Rivest, A. T. Sherman, Randomized encryption techniques, in *Advances in Cryptology: Proceedings of Crypto 82* (1982).

7. B. Schneier, The Solitaire encryption algorithm (1999), available at https://www.schneier.com/solitaire.html.

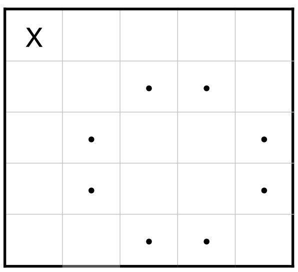
8. C. E. Shannon, Communication theory of secrecy systems. *Bell System Technical Journal* **28** (1949) 659-715.

9. C. Wetzel, Can you behave randomly? (1999) available at http://faculty.rhodes.edu/wetzel/random/intro.html.

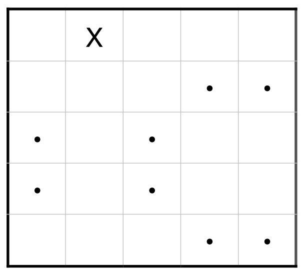
Appendix 1

In processing the n-th character m_n of a plaintext message $m_1 \dots m_{n-1} m_n m_{n+1} \dots m_N$ some combination of choices made in Steps 1 and 3 of the core encryption algorithm will generate a $\sigma(m_n)$ satisfying all the restrictions of Steps 1 and 3, provided that neither $\xi_P(m_{n-1})$ x $\xi_P(m_n)$ nor $\xi_P(m_n)$ x $\xi_P(m_{n+1})$ equal 16.

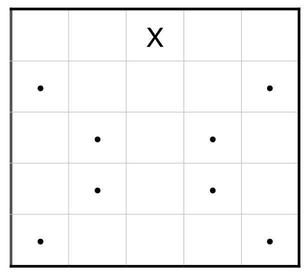
It is fairly straightforward, although somewhat tedious, to show this by considering the distribution of colinear and non-colinear characters with respect to any given character in the 5 x 5 matrix M_K. For any such character the remaining 24 characters comprise 16 colinear and 8 non-colinear characters which can be diagramed as follows, where the symbol • indicates the position of a character non-colinear with the character located at X (see implementation note 10.2):



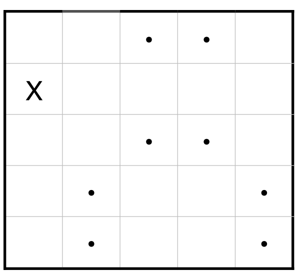
D1



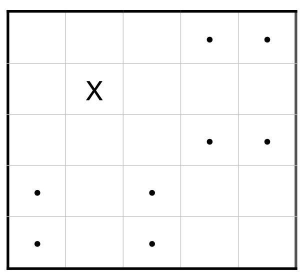
D2



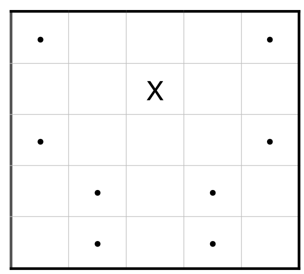
D3



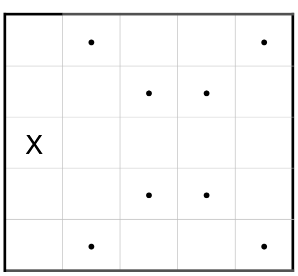
D6



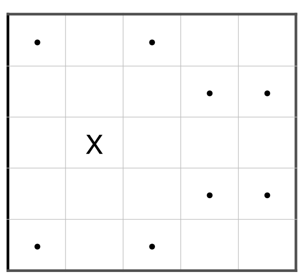
D7



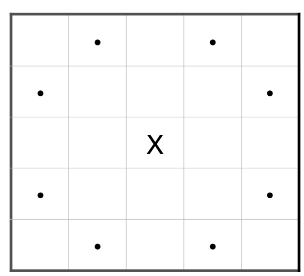
D8



D11



D12



D13

The other 16 possible locations for X result in six diagrams (D4, D5, D9, D10, D14, and D15) horizontally symmetric to six of these nine (D1, D2, D6, D7, D11, and D12), six diagrams (D16, D17, D18, D21, D22, and D23) vertically symmetric to six of these nine (D1, D2, D3, D6, D7, and D0), and four diagrams (D19, D20, D24, and D25) centrally symmetric to four of these nine (D1, D2, D6, and D7).

We prove the assertion inductively by describing an iterative process which chooses a $\sigma(m_n)$ satisfying all restrictions and also "looks ahead" eliminating the choice of any row which would make it impossible to encrypt m_{n+1} when $\xi_P(m_{n+1})$ is a power of 2.

Initially, for n = 1, any of the 20 lines of M_K can be chosen to encrypt m_1, unless $\xi_P(m_2) = 2^k$ for some k, in which case row R_{k+1} is eliminated, or unless $\xi_P(m_1) = 2^j$ for some j, in which case $\sigma(m_1)$ must be chosen as one of the five characters in row R_{5-j} and clearly this is always possible unless k+1 = 5-j or j+k = 4, i.e., $\xi_P(m_1) \times \xi_P(m_2) = 16$.

In general, for n > 1, taking X as the location of the last character of $\sigma(m_{n-1})$ in each of the nine diagrams, it can be seen by inspection that for any of the 31 possible values of $\xi_P(m_n)$ some permutation of the required characters in some line can be chosen to encrypt m_n satisfying all restrictions.

For example, consider the case in which location X is as in diagram D7. Expressing $\xi_P(m_n)$ in binary as abcde, and assuming n is even, in order to make the first character of $\sigma(m_n)$ non-colinear with the last character of $\sigma(m_{n-1})$:

I. if a = 1, one can identify these eight lines: R_1, R_3, C_1, C_3, D_2, D_4, D_7, or D_{10}

II. if b = 1, one can identify these eight lines: R_1, R_3, C_1, C_3, D_3, D_5, D_6, or D_9

III. if c = 1, one can identify these eight lines: R_4, R_5, C_4, C_5, D_2, D_4, D_6, or D_7

IV. if e = 1, one can identify these eight lines: R_4, R_5, C_4, C_5, D_4, D_5, D_9, or D_{10}

If two or more of I – IV are true then some permutation of the required characters in any of those identified lines (except any row which is eliminated by looking ahead at m_{n+1}) can begin with a non-colinear character and therefore satisfy all restrictions.

If just one of I – IV is true then $\xi_P(m_n)$ = 16, 8, 4, or 1 and the required character in either of the corresponding identified columns is non-colinear and can be chosen for $\sigma(m_n)$ satisfying all restrictions.

If none of I – IV is true then $\xi_P(m_n) = 2$ and, by induction, it can be assumed that R2 was not used to choose $\sigma(m_{n-1})$ and so any character in R2 other than the one at location X can be chosen for $\sigma(m_n)$ satisfying all restrictions.

Appendix 2

Given that $|C'| + |K''| \geq 500$ and also $N \geq 30 - R$ where $|C'| = 31 \cdot N + R$, $0 \leq R < 31$ we show that $j \leq |C'|$.

$|K'| = 97$ after transcription, therefore it may be safely assumed that $|K''| \leq 500$, and so $|C'| + |K''| - 500 \leq |C'|$.

Therefore $j \leq \lfloor |C'| / 31 \rfloor \cdot 30 + 30 = N \cdot 30 + 30 \leq N \cdot 30 + N + R = N \cdot 31 + R = |C'|$.

Appendix 3

C_1

```
6EOU, GHP.0 RZ95E MO9.? CBH6D L9PGI Q,MAU J5K.W GT-LC 2FSZM NOT2O SDBPU N4V.A
Z9WRL 8K?N7 ,65X- Y0KMO ND?H8 2BROW -D7TR FWUHA J,-3G Q4RWF SH9O3 4KR5D 3UV,J
KWHWV 0.S5O ,YGL3 F8J4N AU5MT HOL8R A03WG MAK,S 0I753 HRQKO AVF?M 5-RK? QSDX7
VZ683 1PG-4 3,Y9. M2DNQ HJG1E USOV6 LY,AG ?10X2 GUH.G RX5U7 P4VF, 3-G2X 73DZA
CIUNZ O8W6V J5Y3D ?C7K0 5IDAB ,8XCK .N24Z A4IT1 3CJE7 .0TXH VQ4WN .EG.I B3PZ2
C4,S9 X3D2L OR?M3 P4ESF G1B38 OPGZV 97GSQ A-N0Q RUVMA S70KO EA9R0 PF4MU ZLU9O
IF5VK NLHFC OE64S WR2.1 T4LQC -X8EQ -06W4 -BU27 4FARN WVS7G 41MXZ ?3D4Q W60UF
BW97Z TY8RJ EFA2P MCOQL H3G-V X2DCM RU4FJ B0?PG TR02U VBGP7 JNCZ1 IHEDJ K0O6U
8YDEA 0XW1B PRT6N Q-0I2 Q?RZS A97Q4 ,Y-.G 4.AND C.SYU 4BH70 R2PXQ ?M81X Y9KH-
?,.WL 4DV.- FXSCD POG3- 1YD9Q NM0M. 4J8ET ?045X ZCL4Z B2TNJ XW4QX ZY.RV SM3KX
JSB-L COL.D GW3V, RPKDZ VGH91 43A-S PWXG. V,ZKQ 1JYN0 A6GBA .PMS- CF?6H RO?IW
JH6-O TWRMP H?JQ0 P3TSZ I04A8 53FQP WT0DI 3E?Z4 W6831 GPJ-M YA0PJ HJTVH DYAJF
M-C2M 0?GKX ZT,PA WMNXS IT49D .4LG. OJS,Q XKHV. UFQG, DXPJO GD.S- M,4BK Z-X4P
9BHTU O5-PA 5H3B9 ,FHGJ 31K?V 9IN8B JA7M3 4MQJR .0E8L F1CN6 0EVA. 1ZWFN H9OEV
1MH5Z CYN-M T05QZ NSR0O U?Q41 30,TK 5J78I PVTM4 Z2UZE AIV.O Y,JDA ZNFST X51,V
LD.9, 4KW0I 2?0G4 COC13 I5AZ2 UQ,A3 1M-54 PX9I8 NDRJ4 SK3TW QJM.R 2HGKZ 3ISFM
3P8QJ KM9G6 3N90K IC3HE -XDY4 3BMLC F-WA5 XDE5X 9F1L2 BY-D. ?VUK0 OKHFZ VPY-F
CDPBT 5QGH3 RQKE2 V0SQ8 GB35T U0RFP W7ODU B13J4 AXP9, P5D-B .A?6V INO5M FQ6N0
9-Z0G 4UZJ5 QFDQ- TN9O0 BD8R. M?3W- 7?Y5M C.IUP TQ13Z 93,EX H0.SG LI7NQ JW5T0
VHSAV ET23F GBYND ZKOFE XPI3P ZDM6F P?4Z- 5U-2M C5FGS .9OA6 U4ZRK 704VQ L9WFD
SGMYB 96UE1 ?89YP G3OG1 TX.0E DYMSY PG3XS ALRIC 3ZAUI QP?.I TSC45 HTV2S 0Z?QZ
7PH2. 0TU,W RBJU3 ?IOAR STUF0 H2OR- Y8VA7 K,?R, UK0PI MZ3G3 X7K0C REL09 PN,YM
TBY18 7PR0. 53NQ- KZJ2- 1LF5Y ?OJVM RNY7W 0N6JF I,FLK S3.1I PVL21 CQ.VX KWAR-
,4V5I 17H8Q GDTR4 H7E03 X-P,2 BGKCS ,QADG ,MDPO M2GUE NS.0K X74A8 6GKU2 WYCJ-
MPMF. 4CV5X 4UWX1 7RGP. ,MAZ3 IW-GZ 1?SUV MBSO8 A7OX. GJLIW RTOWP HQ3RX 1DK29
,POTG EO64P -,HAZ 3UB2G 47RZM 537NI DSV2E QHGVI 24RZK MDN0K C,ZS5 1Y0?T 4G7X4
ULY3H 4SOJY 9EBFT U1N8S 5YIXA 70?EL TM0HP AF4SC 3EB7- AFXCA NDKFZ 8Z1XB DECO2
VZFNK G.FAO YQ6H0 OSLXT J01BU S,TR? U2WGD H51.B YGA,R J4DIS N75M- AED?K -NMP3
XKD.? 60S5R EQ6SM K3.V? 0.?7J KY2W3 XKJ.? .8E0G M847B ULO8H LD0RM 6T-7W RUF?G
OU439 -,1WY D0AC5 BGQ?A G7JDF RZFT9 SH.A6 ?NHYR 48WCZ ET-D2 YGJO, S-QWD 6NR5V
09M62 ?K9HO A6UB5 V3ZU3 4,-PK 8H?QN 0S9XC WMF2H RM?F4 UPLMA 72C-Q R.YKI 3ZR0O
Z2A-C F5JW3 TQK4J 53WAU RV4WQ 79MX5 31KSP R7RF9 L61PV BEO4N .5269 H1CYQ 3RTZ3
LTFJT QPX-5 064?G N.42Z 4O,GT R7UWH 135QV K17VQ 0W?F3 6SLJM 2XKU, C90?F NSOAJ
WBMKZ I,170 ZY.7W 5HPCR E105S IG9,4 ORS6R PD?UV 05EMO 6YUN4 2,IJF L8PK9 ?3-ZG
?3WAV Z8N9? 2D1,J Y39G3 O.GX, 16TF. DMG7- W3TX0 4HVZD 9AQ?4 ZGSMB Y78I0 ?TU9O
QL?.T SZPEG BUAH5 QIJA4 YNV2O UT8AE 9Q0Q6 ,V01K 4D9BW F15NK H?J2Z 8?BK2 STWHO
JFQYT POB2P LCY86 1T,8. SJP?U OMV0G ?SU0I 1-VJR GPQ8E HRDN, AHJPF 3GW93 -KRD1
V2NH3 MT9-7 ?WC1S BVT54 .I5-? N2E.1 4CLYH XVWP2 6XB20 RZ04V Q.ZCJ EIKZX B12?S
Y8TA4 2DY.D QGSDJ N6GLV O4YDG ?MPQG 5X7QZ 4VW0I J3YC. ?HPH3 B-E4D .QD5R V1X.A
WMYHT PYD5K -B0HN LM,.S I?3ZV TUH69 AO4B3 ,Z3SY NP6Z9 LKNOT V0?DS C.?HL E-W53
PV1,S WZ371 YIJ,F 3?XP. S0A?G CH3TJ ?M.VW 6,SYO 1.ZVI XE.WA 4DXQU I2RO7 MLD5Y
JZQ8Y DFS35 X6YGN 0Q6KP 0DIOQ J9CPF L-73X CZVRD WKT49 CJHL- XMOD. G1L6H XEAO0
GM4IP ,4UFH W.U?W 9OKTL 4DFCX O9KSL .5DTA 7XUE2 S?TCH KAQGU 5K4I9 8?EJK .F68X
407UZ H5M,R SFZSI OJ,HI 1QV8R XTGNW E3Q8P V4J5J ,-MD2 CBUSN FWVLR IO6V- 97AHJ
?6W?I ECOJQ IJ,-4 P2PGY N.RWM 34,PS I7LCG 6FRIX W6?08 O5,WH ?DEN0 1-Q,P SDTG8
YVH0U N2Q,T VRA3Q OSUHO .RPI, BTC?H AQ9CX -8HUL N4?MF 8IAVT LXJC8 R3R2I JP6Y?
KFY7H S?ERH ULSTB CH?0? SDOQX CM.H? WRC97 ZTS.D CHD4K MEVWY L8BKJ ZGIX0 ZUH47
2BWTG QC,RS KZI0A 8KT.5 CUO9O KG6PQ U.?JN E56?N PY5HQ XM60W P7X3F 0RI7V 8Z?PG
DO16P STUEG 2SI.B N4C2V PF8I7 NX?P. ZVQXW Y1HB7 D9CUZ WJKYM CM9OA HE5CT WZB6S
D8FGN ZO3GD 0YHRX YVGRG D.-2X 01LRN B0TWD Y-8BL R7SDY NIXW. TL?5. 8493U F5J9U
S-L2Z H9WML B712Z Q5D3K YRO?3 -H1,R AT54Q 7J9I? O7G2N FTK6Y MUOA0 5BSXK A6M?S
PCGIH U2,U0 2YVLJ 7?PA.
```

(3335 characters)

C_2

```
425JG 8P-,7 .G8H4 .0XL8 OHBD5 CVESV D1YMN .DE61 TWJ-Z 0XZO6 Q9CY1 ZC.P? 7XJLH
W-TBP ?YZ-M 3NVN? 6MUE3 -KR5? G4F?6 8AMCI YR1D2 N?673 UWN5Y -.0F. DBYM6 N8FEH
V34,Y SCTU7 IZX3S KZ-FY ,R8.? 0OBUT 2-JM6 ZWV3M AKXJ2 NW2Y? 7MZ8F 240UI .LV9Z
5EUND A-357 MFK4L PB3KN GR-1U 37N6Y MW6OS NFLSN MKN?6 X7UJD E?Z85 Y1K02 ,D.4G
M0.YV PS0EH 7.CVO 0XJD. -Z9?P LNEDK YO1MC Z0H-O 3E67? H-.O, Q8RSU K5A,6 0JNB0
8G1ZA 4.,MD HA52A 47YGM .6DU4 L5.T3 ,6ZR7 MB3AL 7?X0A 42,XW KTOYG 5DZFL 02J1E
P4,T. 85VHY QFQCO EP9W0 H,?JD 457LB -VAEG 4QIWP DIF1A 3SK,V -SDJ? G,Y87 TD156
31SWM TU,5K -TNDX TA163 IHDCZ VXRJU XN0-D KW9CX GN-AI ?,J3N D-V64 169U, PTWX7
K438F CD3SG ,VK-? E1N6X QU9-L G1Y3C FOVUR P-X4L FPOJ, 2Y?ED UXM56 -,UAT SQKOA
YTO58 1XMVS KF1S4 XRZTQ J,-8Y X9F46 A,B-R ?HPA8 3SMO2 LVSPK X5IFK L05BR CA8ZB
.OIWT DGSV3 W9XHR XFWHS 9MWYR JCK6N 5UVT1 ,HF., 3H5A2 F434N GA.R? V,7ZK MP1N3
H8PIT IQ?14 CNVQL 491O5 ST,GA 3FVYM G?I90 N67KQ J0GI9 XEBR3 ?QMD, OSBRL G5?3S
B,9L7 4B.Y, QA7O8 40QTU CG1PZ KYV7? PB6EQ FB8MG -9DZY R-0JA U1.NH LP,5U V9TPX
B3O0W DKIAJ M13DG IF4GE 6GHC1 T.XG7 2L?E4 NUX82 YBFGC YAN95 8YVN2 8OKV- 36I,9
WXZ79 OM3QH 98E?- NAOHV W54LA N0IEZ 9LU7X E6D3G TH-W3 4XW,1 08OHK T31?M S2R6J
57V-Y ZHC2F .4BYU ZEQUR X7AVP OFH-L 1ZS,9 N-AHP 4D?6O 7R3BW 9FE02 46L3M C9PU,
KH-DB L5WR9 EG-D3 O6.V, PITOM Z6YIG TW7RS 3YR91 6WDCL 7ANTJ IG2.D 8RK9P N05SO
6RU8K 2CQZW TYD0N 1M2AH 089RO EDP6E DSHNU .1QC1 A8JY2 DAGQK 8PU31 7E69D 825SK
G-ZL, E.8X5 FBVME VT8LJ MEP6Y IT185 68IEO NUFKA 8VE2D C4LWE 8PM6F 4S0BF 6SI3-
1PU9E Y0C,0 9BXEY Q9F.C MK?., E3ZH. I9-1F DAC9O 6TKJ9 7FVCY ,N1UL -.JXC R3A9Y
4-?SL OZ5XY 58FI4 SG6H8 9KFPT YXIJL NOQGU 6-713 O24FL XZ,CA 3YKYS M,Q0T QGJF9
D5,KA Y3FKM 50UQ8 NMV3T ?9PAB W0EQL CR74Y V1-G5 E31MK RYV?Q EO2R3 UNE69 G04?7
-MI?2 KZ8S0 -B5I1 C2DHK OQ071 QNXWQ EBH?A -XJ.I FSCZH 138.R IEQUB VA0YL S8B6T
5FM7R GUHCA ON,7L J9LS8 162UA EBK4Q 318SY X,E7D BJ1FN ,6MG9 XDY3F .HYC3 J0XR.
BFAM5 9B,0X O1JTY -4-OW 2LJ3W 9DB2R QYV?X 0W5C0 LH281 9LJDX V-Z2. XLWJV CU7-C
UAHD. ABL52 ?U0TA QBHO8 UYEPR K76IN JUHC? 27QBH X52.3 G.7,Y JUQ,G 5ZGI9 -12H8
N9?-D 4U0EH CRXZ, ?08.4 A35MV XPS6O F7GK3 0E?PT NQBW3 97C-? 47EIM .TKVQ M1J76
WUIDR BVY.J D6MQ8 UZH0C .ED1- RUGDB ,7961 89AZD .8R3P QHWLB V5WJ6 CYMTS PBOQL
CM7B6 ZXW98 49RNH TVYU? 0PXIE NL1QJ 3?5FI PMC5L 068T1 F4X3- 1K8C. HYFL? PXW,O
TPM9D BXZ-O N9UT0 ,5PG1 4WVH3 WQY.G 7BDK5 0TP,8 ADZBJ W6OH7 1L?3S 7LZDK U,MW8
0BZ2L -58JO ME3QK BCNRQ PJOFV T17?S L-JI2 X9Z-I .OLJZ MB-4D Q?APK M?5AP MNXY-
J2?UG ML?S5 KZ.IG CX5MJ LF6D4 CH.BZ 3OOUT X46OF SHZ.C 8MB9G BFOJ? XMP,E B3VM9
LPI-. ODJDX 3G1TG L?6AF 2-Z96 WJ?,J E2A1Y 47F-Z 9?Z,2 8POL5 C3L7? XT1QJ T7.1-
UGXO4 D-FJE S,5?L R7857 JPWEM .A-HG JT,07 ZFY3R 7FNTA LS-2F BP8V6 7N7,R CKWOY
95XLE -RSOX UFY10 T3HN5 MYUG8 29HM. DIYNI 7TNIE ,1QZJ AY-JT H-MOF 5HNLR ECI0B
PAQKJ G6?4W EGZCH YJA-T 9DIP8 H,D8. -Y56N R24UC .ZAOY 2EBJ0 1DK6Z 9Q5JV I8DXP
J0I2G -IWN? C9F1. EYMSC NH7ZR 456CD S-QLV TYM7A -L94S 6OD2N C71HQ 0PY58 EL?UH
CSK,Y 87SZT 5DCBF 7Y93H ZC10- XRSDZ 0E9-D 7TMGX F.VOW QSGE8 RK.JX 4AP78 WX1I.
7YAWV F935S NE?YB PKJ6Y 9FKRW 6H5X7 T4,.Z ,?82D K.XLH 52PNO JEXVT 843SD PMOIY
LIC4X KP6JI 9YFW6 KX9W. 4,U3X SYM,K X-,Z7 ?E6KN T1A7E CS062 013YF -LS7C L5Z,J
NSL1B 2U-JU OGTIX 32QLV .31UF 4N6EX FHRLS 8RMBS L0ZKA QP3?S EMVY3 IOQ.8 6IMBH
P?Q-, 5VKQX U6OR0 QI7GQ PE.CZ TX50I FHL-? LT13M 9H0B3 RU8I? B0M,1 U4SZU H93XH
GELZD GBFIW A?I7Z ,L69V DAJ4N MFE8Z EW58Y H6RK0 98?WJ NM9U? XWNUF DAI6- WFRS1
NPOCV IB4CL K04RI YKAUH O4W1K BSN,C VLREV 3975W H?X63 CFWU5 IKS-G D.FO9 CK7D4
QSX8I 3HOLQ 7,V-, I4P,? 251YF 3AKUJ FJIX0 YKAUI ZAQ8S XN-HB T?Z2. F1.SG RZKMI
7?U62 70YJE QWP.I ?X3M? 5LX3. A4W1J P6Y?K FY7HS ?V3Q6 WRTPD ?B5N6 KQDM- F6TW2
BJDAX 6EHN8 A3LZ? SHWP9 80AI? 6DQW. DOO8R TI3U0 ZH48I 9HTRP SWZFV ,A.G- Q5JC8
X?YHC X.VBI ETUDY ,W1XK NB5CO ,?.XA 8J7E0 IDIPE 7YKFT 5ANMC ETRWU .NQZT 14GLD
G,J?X O2.KB ZEH5X 8MS.G XIQW9 Q6GNS 1DF4Q CT93, BAX9D IHPFG X54?R 9OSEL 673H0
D-2AI ?SO-T G9E6P MJVWK XB,A9 65AD4 NELIG HSRCV 0I9Y, XTWD0 YPB?P XL23E AT8?I
DKOLW MT0V0 PYK5S BM0T6 5MIX8 Y6NOM Z3-69 YX834 R7YA- 5VJ,A NO63G -,?
(3308 characters)
```