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 reasonably 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 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 [5] 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 is theoretically possible 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 [6] 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 small key (34 decimal digits), Handycipher incorporates a nondeterministic encryption procedure along the lines described by Rivest and Sherman [4], and employs multiple encryption as suggested by

Merkle and Hellman [2], as well as a randomly generated session key for each message. Combining a simple 31-character substitution cipher with a nondeterministic homophonic substitution cipher that uses a cipher alphabet comprising an enormous number of tokens 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.

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 omitting the space character ^. Some permutation of the 31 characters of A is chosen as the secret shared key K, say for example,

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

and the 30 non-space characters of K are displayed as a 5 x 6 table, T_K

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

and the ordering of the 31 characters in K is displayed as a substitution table, ξ_K

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

Then, by referring to T_K and ξ_K, 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 two principal diagonals, each plaintext character is encrypted by first expressing its position in K 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 that character with a subset of the 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 A occupying position 19 = 10011 is encrypted into one of the six permutations of one of the twelve 3-tuples

{L-F .RH GSK AWZ M,Y LAM CIV PBN -W, FZY LWY FIM}

whereas the the plaintext character J occupying position 15 = 01111 is encrypted into one of the 24 permutations of one of the twelve 4-tuples

{CP-F Q?RH UJSK IBWZ VN,Y .GAM QUIV ?JBN RSW, HKZY QJWY RJIM}

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

A plaintext message M is encrypted into a ciphertext cryptogram C by means of the encryption algorithm E defined as follows:

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

First, omitting ^ the remaining 30 characters of K are displayed as a 5 x 6 table T_K by writing successive groups of six 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_2, R_3, R_4, R_5, C_1, C_2, C_3, C_4, C_5, D_1, and D_2, respectively.

Also, a simple (numerical coding) substitution ξ_K is applied, transforming each character m of M into the number $\xi_K(m)$ representing its position in K (i.e., if K = $k_1k_2...k_{31}$ then $\xi_K(m) = i$ where $m = k_i$).

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

1. A random choice is made between:
   1.1. <u>*Column-encryption*</u>: One of the five columns in M_K, say C_j, is chosen at random, or
   1.2. <u>*Row-encryption*</u>: One of the five rows in M_K, say R_j, is chosen at random, subject to the restriction that $\xi_K(m) \neq 1, 2, 4, 8$, or 16, or
   1.3. <u>*Diagonal-encryption*</u>: One of the two diagonals in M_K, say D_j, is chosen at random, subject to the restriction that $\xi_K(m) \neq 1, 2, 4, 8$, or 16, or
   1.4. <u>*Null-insertion*</u>: A so-called "null word," as defined below, is randomly generated, a flag is set, and Step 1 is restarted.[1]
2. $\xi_K(m)$ is expressed as a five digit binary number, $b_1b_2b_3b_4b_5$, and
   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.

[1] It's a fairly straightforward exercise to show that null-insertion is only forced when $\xi_K(m) = 1, 2, 4, 8$, or 16 and $\sigma(m)$ must lie in the same row used to encrypt the character immediately preceding m in M.

3. The elements of the subset specified in step 2 are concatenated in a randomly chosen order. If the flag was set in Step 1, the string is prefixed by the chosen null word and the flag is reset. If this string, composed of 1 to 16 ciphertext characters, satisfies all of the following three restrictions, where $\bar{m}$ denotes the character immediately preceding m in M, then it is taken as $\sigma(m)$. Otherwise, Step 1 is restarted.

   3.1. If $\bar{m}$ was column-encrypted then the first character of $\sigma(m)$ must not lie in the column containing $\sigma(\bar{m})$. If, in addition, $\xi_K(\bar{m})$ = 1, 2, 4, 8, or 16 then the first character of $\sigma(m)$ must also not lie in the row or any diagonal containing $\sigma(\bar{m})$, and
   3.2. If $\bar{m}$ was row-encrypted then the first character of $\sigma(m)$ must not lie in the row containing $\sigma(\bar{m})$, and
   3.3. If $\bar{m}$ was diagonal-encrypted then the first character of $\sigma(m)$ must not lie in the diagonal containing $\sigma(\bar{m})$.

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 = $\sigma(m_1)\sigma(m_2)\sigma(m_3)$... 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 characters contained in either the same column, row, or diagonal of M_K —stopping at and discarding null words—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_K.

A null word, as used in Step 1.4 of the encryption algorithm, is defined as follows:
- a *null character* is defined as any of the five characters comprising the sixth column of T_K
- a *null prefix* is defined as a string of n distinct null characters, $1 \le n \le 5$
- a *skew chain* is defined as a string of n non-null characters, $3 \le n \le 6$, in which no two adjacent characters are co-linear except the last two which must be co-linear
- a *null word* is defined as a null prefix followed by a skew chain (hence a null word has length n, $4 \le n \le 11$)

Thus each plaintext character m is encrypted by randomly choosing a row, column, or diagonal of the key matrix M_K and representing that character's numerical code $\xi_K(m)$ by an n-tuple $\sigma(m)$ of characters lying in the chosen row, column, or diagonal. 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 same row, column, or diagonal chosen to encrypt the previous plaintext character nor is it allowed, when the previous character was encrypted as a single ciphertext character, to begin with any character lying in any row or diagonal containing that previous ciphertext character. Finally, the five characters lying in the sixth column of T_K may be used to generate null words when required to demarcate successive character encryptions.

With any key, and ignoring the addition of null words, of the 31 characters comprising the plaintext alphabet A:
five are encrypted into one of 5 length-1 ciphertext unigrams,
ten are encrypted into one of 12 x 2! = 24 length-2 ciphertext bigrams,
ten are encrypted into one of 12 x 3! = 72 length-3 ciphertext trigrams,
five are encrypted into one of 12 x 4! = 288 length-4 ciphertext 4-grams, and
one is encrypted into one of 12 x 5! = 1440 length-5 ciphertext 5-grams.
Taking into account that each n-gram can optionally be prefixed by one of N null words, the number of possible cipher tokens is seen to be:
(5 x 5 + 10 x 24 + 10 x 72 + 5 x 288 + 1 x 1440) x N = 3,865 x N, where N is a very large number. (There are 325 possible null prefixes, 2,146 possible length 3 skew chains, etc.)

3. Example encryption with the core cipher

Although any permutation of the entire plaintext 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, omitting all duplications, spaces, and non-alphabet characters; then ^ and all other alphabet characters missing from the resulting string are appended in reverse order, i.e., in the order:

```
{^ ? - . , 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 (perhaps, as a plot device, identified by a secret agent's whistling the melody) 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 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

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

The substitution ξ_K 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_K(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	13	01101	DA- NTF	SCZ SMY	MVX CVR	KEQ HU.	YRJ ZXJ	SVJ KV-
B	31	11111	ODAI- ONTPF	NSCHZ DSMKY	TMVUX ACVER	PKEGQ IHUG.	FYR.J -ZXQJ	OSVGJ FKVH-
C	14	01110	DAI NTP	SCH SMK	MVU CVE	KEG HUG	YR. ZXQ	SVG KVH
D	7	00111	AI- TPF	CHZ MKY	VUX VER	EGQ UG.	R.J XQJ	VGJ JH-
E	16	10000	O	N	T	P	F	
F	5	00101	A- TF	CZ MY	VX VR	EQ U.	RJ XJ	VJ V-

etc., where, in each row, the groups of characters comprising the rightmost six 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 twelve triples in row 1, B is randomly transformed into one of the 120 permutations of one of the twelve quintuples in row 2, E is randomly transformed into one of the five characters in row 5, etc., subject to the restrictions specified in steps 1 and 3.

So, for example, the plaintext CATS AND DOGS can be encrypted as follows[2]:

[2] In the fourth column the row, column, or diagonal chosen in Step 1 is indicated.

m		**ξ_K(m)**	**C/R/D**	**σ(m)**
C	14	01110	C_2	CSH
A	13	01101	C_1	AD-
T	3	00011	D_2	H-
S	8	01000	C_5	Y
^	24	11000	R_3	CA
A	13	01101	R_4	.HU
N	2	00010	C_4	BLWNMHZG
D	7	00111	D_2	-HV
^	24	11000	C_3	TM
D	7	00111	R_1	?,-UCSPFT
O	1	00001	C_4	Q
G	22	10110	D_1	VGO
S	8	01000	C_3	M

yielding the ciphertext

`CSHAD-H-YCA.HUBLWNMHZG-HVTM?,-UCSPFTQVGOM`

Note that `-H` could not have been chosen instead of `H-` for σ(`T`) according to restriction 3.1.; similarly, `K` could not have been chosen instead of `Y` for σ(`S`) according to restriction 3.3. The choice of R_4 to encrypt the sixth character forced the use of a null word for σ(`N`); the use of a null word in σ(`D`) was optional.

This ciphertext would be decrypted by dividing it, according to the table T_K, as

`CSH AD- H- Y CA .HU G -HV TM PFT Q VGO M`

(dropping the null words `BLWNMHZ` and `?,-UCS`) and then finding each group's associated binary number, converting to decimal, and decoding by inverting the substitution ξ_K

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_K^{-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 229-character plaintext

```
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
burns you. But I think the spirit of man is a good adversary.  -- Tennessee
Williams
```

which can be encrypted by the core cipher in a great many ways including, for example, this 990-character ciphertext:[3]

[3] The ciphertext characters are displayed here divided this way for clarity of exposition; in practice, of course, they would instead only be customarily divided into groups of five.

```
Q-J ,LXCUZXG. OS B?WEOS-X B?L-NY-SGYMS B?,DEHTGUJ-X H QG WL,?CDJEAM -Z FN
?LBWAQEF LVPMQCNHU NO XU AV LB?ZADF MT R KEQ S ?LWFUCF.Y VRC HVF T
?LWBGRCCA X CZ BHASQDMZ- RE GOJ L,BATEDMQK N ARVE ?,WXIM-HAC I.G PK
LB?IFQXGQ RF OPF . SG TM RE KYD ?BKZGRDMCR O LWB?VIGIH LBW-NXISCGQP
,AUE-ZK W?B,CXT-Z BWXYICHD-A YF MX O YD WSFDHCDIA LVQCUIPOF HV N M
?L,QMJCHY B,EHEIOTM PF B-G.AO EAR G ,W.OFQX- VRAE FK B?S-YNUGJQ- DS GJ X-
IG. ,BW?DHEJI-H QZ TM CH FPO QE T SD PQG S TM KV- MT C ?,OUA.UXT Q
BUQSRFHCS P L?,WBHDCEM ?LWKXAFUIK Z- BLNXRPSYJ WLGAYIZJJR TM LWZEMKYJR.F
ARV FO B,L?FEYEKI JQ- U FHV NO - ?,LB.V-U O ,VIOY N VG XV NS - W,BAJERIU.
QJ FY -KV U JVG NO -H REA -D N AC B?IZXZHN LB?UYRK ?LBJAMTCA H-
?LBHOXCZTV O B,CPAQGKP V- XTU YD F AC LBW,OQPPF VT QEK J. B?WSRQPYF
?BLJD-PTONF U.I ?W.XKCSI. ,OMFE-JG W,YNANSY AC QJZ B?WHP-TR.Z I.U OJGV
W,B?ZFNKP BW?L,QCFZX-DIAO FOT W?LBKRTDMHZ FK .JF Z- KY X- ,WOZDRMSFJ.
 H L,BWPZQZQ ?WBNEODDS ER PE N YF M C GI. PQ -FH YK Z- ?,RIQVFX ?WPY.CZ
DS -D RJY G YF -JQ K AC FNT YF -QX WL-PKX WLBSINHQ ,YQVZAO-IA MT JSV UG.
QGKE N WL?UKMFJ S XZJ L,P.-NMSTX REC FOPT IH ?LBQUNCFY CAE KGP TM G. N
BW?IRPQ. L,?XSNH T K ?WPXKQM O ,OCO.VKT HI ?BJKNEZQGI BL?N-TPI.G KM
LW?AYPXOAKM UTX A-D CR BWXSXUM
```

containing 73 null words.

```
I   t         ^  h        a            u            n t  s          ^  m
Q-J ,LXCUZXG. OS B?WEOS-X B?L-NY-SGYMS B?,DEHTGUJ-X H QG WL,?CDJEAM -Z FN

e        ,         ^  t  h  e       ^  p a   s s         a   g   e
?LBWAQEF LVPMQCNHU NO XU AV LB?ZADF MT R KEQ S ?LWFUCF.Y VRC HVF T

^         o f  ^         t  i   m          e .    ^          I   ^
?LWBGRCCA X CZ BHASQDMZ- RE GOJ L,BATEDMQK N ARVE ?,WXIM-HAC I.G PK

t         h  i   n k  ^  t  i   m          e ^         i
LB?IFQXGQ RF OPF . SG TM RE KYD ?BKZGRDMCR O LWB?VIGIH LBW-NXISCGQP

s       ^         a          ^  m  e r  c         i         l  e s
,AUE-ZK W?B,CXT-Z BWXYICHD-A YF MX O YD WSFDHCDIA LVQCUIPOF HV N M

s         ^         t  h      i   n g        .    ^  I           ^  t  h
?L,QMJCHY B,EHEIOTM PF B-G.AO EAR G ,W.OFQX- VRAE FK B?S-YNUGJQ- DS GJ X-

i   n           k  ^  l  i   f  e ^  i   s ^  a   p  r o         c
IG. ,BW?DHEJI-H QZ TM CH FPO QE T SD PQG S TM KV- MT C ?,OUA.UXT Q

e         s s          ^          o  f         ^          b  u
BUQSRFHCS P L?,WBHDCEM ?LWKXAFUIK Z- BLNXRPSYJ WLGAYIZJJR TM LWZEMKYJR.F

r   n  i          n   g ^   o  n e          s     e l  f  ^  o u
ARV FO B,L?FEYEKI JQ- U FHV NO - ?,LB.V-U O ,VIOY N VG XV NS - W,BAJERIU.

t  ^  a   n d   ^  t  i   m  e ^  i        s       ^         t
QJ FY -KV U JVG NO -H REA -D N AC B?IZXZHN LB?UYRK ?LBJAMTCA H-

h          e ^         f  i   r  e ^  t         h  a   t  ^
?LBHOXCZTV O B,CPAQGKP V- XTU YD F AC LBW,OQPPF VT QEK J. B?WSRQPYF
```

```
b           u   r         n        s        ^  y   o          u   .
?BLJD-PTONF U.I ?W.XKCSI. ,OMFE-JG W,YNANSY AC QJZ B?WHP-TR.Z I.U OJGV

^         B               u   t           ^  I   ^  t  h  i
W,B?ZFNKP BW?L,QCFZX-DIAO FOT W?LBKRTDMHZ FK .JF Z- KY X- ,WOZDRMSFJ.

n k         ^         t  h  e ^  s p i   r  i   t  ^  o        f       ^
H L,BWPZQZQ ?WBNEODDS ER PE N YF M C GI. PQ -FH YK Z- ?,RIQVFX ?WPY.CZ DS

m  a   n ^  i   s ^  a   ^  g   o      o        d          ^  a   d
-D RJY G YF -JQ K AC FNT YF -QX WL-PKX WLBSINHQ ,YQVZAO-IA MT JSV UG.

v    e r        s a   r          y   .    ^  ^         -   -   ^  T  e
QGKE N WL?UKMFJ S XZJ L,P.-NMSTX REC FOPT IH ?LBQUNCFY CAE KGP TM G. N

n        n       e s s       e e        ^  W          i          l
BW?IRPQ. L,?XSNH T K ?WPXKQM O ,OCO.VKT HI ?BJKNEZQGI BL?N-TPI.G KM

l           i   a   m  s
LW?AYPXOAKM UTX A-D CR BWXSXUM
```

Although the average bandwidth expansion factor apart from added null words, averaged over all possible keys and all possible messages uniformly distributed, is

(5x1 + 10x2 + 10x3 + 5x4 + 1x5) / 31 = 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 x 0.28 + 2 x 0.45 + 3 x 0.23 + 4 x 0.02 + 5 x 0.01 = 2.2

while that of this particular encryption is (506 - 38) / 229 = 2.04.

4. Handycipher

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 the core cipher using K′ to produce an intermediate ciphertext C′. K′ is then encrypted with the core cipher using K and embedded in C′ at a location based on K and the length of M, producing the final ciphertext C.

Extending the core cipher 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.

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

1. Generate a random 31-character key K′ with associated table $T_K{}'$ and coding substitution $\xi_K{}'$.
2. Encrypt M with the core cipher and K′, yielding C′.
3. Encrypt K′ with the core cipher and K, and append a null word (from T_K), yielding K′′.
4. Compute $j = \{\lfloor(|C'| + |K''|) / 31\rfloor - 3\} \cdot (\xi_K(\mathtt{U}) - 1) + \xi_K(\mathtt{F}) - 1$.[4]
5. Insert K′′ into C′ immediately following position j as calculated in step 4, yielding C.

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

1. Calculate $j = \{\lfloor|C| / 31\rfloor - 3\} \cdot (\xi_K(\mathtt{U}) - 1) + \xi_K(\mathtt{F}) - 1$ and begin decrypting the substring of C immediately following position j with the core cipher and K.
2. Continue until 31 plaintext characters have been decrypted, yielding the session key, K′.
3. Remove the decrypted substring from C, leaving C′.
4. Decrypt C′ with the core cipher and K′, yielding M.

5. Example encryption with Handycipher

Continuing with the previous example, to encrypt the Williams quote with Handycipher, at first a random 31-character session key K′ is generated, say the one used as an example in Section 2:

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

[4] Here ⌊x⌋ denotes the integer part of x and ICI denotes the length of C. The formula is designed merely to make the value of j depend on K and ICI. (The choice of `U` and `F` is arbitrary and based on their central position in the usual frequency distribution `etaoinshrdlucmfgypwbvkxjqz`.)

with associated table $T_{K'}$

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

and coding substitution $\xi_{K'}$

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

The quote is then encrypted with the core cipher using this $\xi_{K'}$ and $T_{K'}$, yielding, for example, this 906-character ciphertext as C′

```
NMYDE XO.B? ZAIJL KSUBP N,NVK HFTXE VAYPR ,.LMF NMRFI .RPNJ ?FJ.H Q,WRM
,JLOE J.YSG KSMY, CTODE G,SFN PBYJQ ZFS-K ZS,FK VCQOX T,LC? H.IFR -WAMG
-SMJF -SQH. YZHMN YHKFE XYGH- BALFT .VJHI RGJTX YC,.Y WIAZE LKIYB PFKYE
ODPIK PF?BP ODTAF ,N-WK FLPFO XHSNU ZHLKF ,YMPJ EOK-Z NJ-RW FIA.Z XOTES
YCKCV LMGYS GTOSC KCMYP OXYR, PABFM RN?B. H?LJQ H?QSW ,BAPN JFKUG KN?BF
YKQUC NPUC, FPLKY M,GJL MGCGJ EOT,Q NWVM, MYDMW ZGLRH ZHJSB TZLFA LEXOJ
VRCBW LOX.W GYFLB AR?JY PLDTE OAP.Y JWBAR WS?BF RJOT- UFWJP NJDB, QKFUQ
CMRJ. ?JBQU CLA-Z F,TOX QG,J, V?HPL IJA.G VQCFJ BNPRJ F.LGM AEDTY RHFKD
OT.Y. HM.LP FLRW- CIJL? .HT.J AYPCP KFMYV SUKPB -SNYF KYRQZ FPLQV CHQRK
SGDTE -NGWY FCLGJ AGLJB ?EDOT BMNWR FKHLU CPB?J IUJSU F-PKF XOA,H RLP-I
UQR-, FKEOT ,?L,F -KFY- SMRFX DILNU VB?NK GJRJF NPGJD EX,UH WFH-R ,HZYO
DEXL, -L-JP CNBKY FSUMG LHQ.J FGAPF MN?PB TXDOY .MZAW JP?KF GJKCG LDOEC
HL?MN -W,MN RMJN, WSYZH FKJFB NPLA. GMTDE WHWMP BCQIV WLC-E TL,.F HFODX
BHSMI ICVXV B.M-C RSW-B ZWFJG LUDXE TOMK- VR-JO DX-V, MNXEC SL.H. QGS-S
RKFHA WCEXO DWC?N LTEOZ PVPLL AFZCU .H?RV CUDOE T.KWV GMMOX D?SL- MBAZ-
,W.LA F
```

K′ is encrypted with the core cipher and K, and terminated with a null word, yielding K″, for example,

XQMUVRQ-ZRJ-EVRAIHU.-FKRATVDMSB?L-NY-SGKMDB?,DEHTGUJ-XVHFK?,V.P
AOSWNMUPNB?LRIPOOQKEHI-IOYJR.FKDPKQGJGQKY.JRUYRH-KMKYW?LBTAHK

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

$$j = \{\lfloor(|C'| + |K''|) / 31\rfloor - 3\} \cdot (\xi_K(\text{U}) - 1) + \xi_K(\text{F}) - 1$$

$$= \{\lfloor(906 + 124) / 31\rfloor - 3\} \cdot 20 + 5 - 1$$

$$= 604$$

K′′ is inserted following the 604th character of C′, yielding C

```
NMYDE XO.B? ZAIJL KSUBP N,NVK HFTXE VAYPR ,.LMF NMRFI .RPNJ ?FJ.H Q,WRM
,JLOE J.YSG KSMY, CTODE G,SFN PBYJQ ZFS-K ZS,FK VCQOX T,LC? H.IFR -WAMG
-SMJF -SQH. YZHMN YHKFE XYGH- BALFT .VJHI RGJTX YC,.Y WIAZE LKIYB PFKYE
ODPIK PF?BP ODTAF ,N-WK FLPFO XHSNU ZHLKF ,YMPJ EOK-Z NJ-RW FIA.Z XOTES
YCKCV LMGYS GTOSC KCMYP OXYR, PABFM RN?B. H?LJQ H?QSW ,BAPN JFKUG KN?BF
YKQUC NPUC, FPLKY M,GJL MGCGJ EOT,Q NWVM, MYDMW ZGLRH ZHJSB TZLFA LEXOJ
VRCBW LOX.W GYFLB AR?JY PLDTE OAP.Y JWBAR WS?BF RJOT- UFWJP NJDB, QKFUQ
CMRJ. ?JBQU CLA-Z F,TOX QG,J, V?HPL IJA.G VQCFJ BNPRJ F.LGM AEDTY RHFKD
OT.Y. HM.LP FLRW- CIJL? .HT.J AYPCP KFMYV SUKPB -SNYF KYRQZ FPLQV CHQRK
SGDTE -NGWY FCLGJ AGLJB ?EDOT BMNWR FKHLU CPB?J IUJSU F-PKF XOA,H RLP-I
UQR-X QMUVR Q-ZRJ -EVRA IHU.- FKRAT VDMSB ?L-NY -SGKM DB?,D EHTGU J-XVH
FK?,V .PAOS WNMUP NB?LR IPOOQ KEHI- IOYJR .FKDP KQGJG QKY.J RUYRH -KMKY
W?LBT AHK,F KEOT, ?L,F- KFY-S MRFXD ILNUV B?NKG JRJFN PGJDE X,UHW FH-R,
HZYOD EXL,- L-JPC NBKYF SUMGL HQ.JF GAPFM N?PBT XDOY. MZAWJ P?KFG JKCGL
DOECH L?MN- W,MNR MJN,W SYZHF KJFBN PLA.G MTDEW HWMPB CQIVW LC-ET L,.FH
FODXB HSMII CVXVB .M-CR SW-BZ WFJGL UDXET OMK-V R-JOD X-V,M NXECS L.H.Q
GS-SR KFHAW CEXOD WC?NL TEOZP VPLLA FZCU. H?RVC UDOET .KWVG MMOXD ?SL-M
BAZ-, W.LAF
```

6. Cryptanalytic vulnerability

Handycipher is conjectured to be remarkably strong for a pen-and-paper cipher, based on the following considerations.

It seems reasonable to assume that any effective attack will be based on determining the makeup of the twelve rows, columns, and diagonals of the key matrix M_K as well as the sixth column of the key table T_K containing the five null characters. However, any such strategy will almost certainly require a fairly large amount of ciphertext to be effective—far more than is likely to be encountered in a typical pen-and-paper cipher application.

The 990-character ciphertext generated by the core cipher encryption of the 229-character Tennessee Williams quotation in Section 3, for example, contains 335 distinct unordered bigrams (i.e., counting both permutations of a bigram as one) of which only 14 occur more than five times; 636 distinct unordered trigrams of which only four occur more than three times and only one of these (.HU) consists of characters co-linear in M_K; 727 distinct unordered 4-grams of which only two occur more than two times and none of these consists of characters co-linear in M_K; 734 distinct unordered 5-grams of which only five occur more than two times and none of these consists of characters co-linear in M_K.

Moreover, even if an attack were to successfully discover the thirteen subsets of A* which comprise the rows, columns, and diagonals of M_K and the sixth column of T_K, thereby completely determining how to divide a ciphertext into its component n-grams, ciphertext-only decryption might well remain an intractable problem. Such an attack would, in effect, only reduce the problem to one of breaking a homophonic substitution cipher with 186 cipher alphabet-tokens (those distinct unordered n-grams occuring in the ciphertext that are indeed encryptions of plaintext characters) and a ciphertext size of 229. Moreover, of these 186 tokens only five (three encryptions of ^: AC, TM, YF and two encryptions of E: N, O) occur more than three times. That such a problem is beyond the scope of known ciphertext-only attacks against homophonic substitution ciphers is implied by the work of Dhavare, et al. [1]

7. Challenge cryptograms

Two 506-character plaintext messages M_1 and M_2 have each been encrypted with Handycipher using the same key K, yielding the two cryptograms C_1 and C_2 contained in the Appendix, not necessarily in that order. The first 229 characters of M_1 consist of the Williams quotation in Section 3. 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.

8. Implementation notes

8.1. When implementing the core cipher encryption by hand it's helpful to proceed by first writing the plaintext message vertically; then adding a second column containing, adjacent to each character m, ξ(m); then a third column containing the column, row, or diagonal of M_K to be used in step 1 of the encryption algorithm; finally a fourth column containing σ(m).

Thus a worksheet might look like:

m	ξ(m)	C/R/D	σ(m)
C	14	C_2	CSH
A	13	C_1	AD-
T	3	D_2	H-
S	8	C_5	Y
^	24	R_3	CA
A	13	R_4	.HU
N	2	C_4	BLWNMHZG
D	7	D_2	-HV
^	24	C_3	TM
D	7	R_1	?,-UCSPFT
O	1	C_4	Q
G	22	D_3	VGO
S	8	C_3	M

Proceeding in this way facilitates choosing columns, rows, diagonals, and character orderings in σ(m) in a random fashion.

8.2. Although the process is tedious, with a bit of practice one can reasonably expect to encrypt or decrypt messages with the core cipher 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 20 minutes to generate, encrypt, and insert the session key.

8.3. For the random choices made in steps 1 and 3 of the core cipher encryption algorithm and step 1 of the Handycipher encryption algorithm to be truly random, one can use a single six-sided die (as described, for example, by Reinhold [3]); however, it's sufficient for our purpose that these choices merely be made nondeterministically since a hand cipher need only be capable of protecting a small number of short messages. Nonetheless, trying to choose randomly can only make cryptanalysis more difficult. One can improve one's skill at behaving randomly by visiting Chris Wetzel's website [7].

8.4. Although there is little propagation of errors in both encrypting and decrypting (which is particularly desirable in a hand cipher) special care should be taken when processing the session key K′ in step 3 of the Handycipher encryption algorithm and step 2 of the decryption algorithm since any error introduced into the key will be propagated.

8.5. Null words should certainly be introduced in encrypting the session key so that its length is not predictable, and the encrypted session key needs to end with a null word to ensure that its boundary is demarcated in the decryption process.

8.6. It can happen that prefixing a randomly chosen null word results in doubling a character in the ciphertext; this should be avoided since it needlessly leaks the information that the doubled character is co-linear with the preceding character.

8.7. Frequency distribution of ciphertext characters could easily be further flattened by introducing into Step 1 of the Handycipher encryption algorithm, modifying K′ so as to avoid $\xi_{K'}(m)$ being 0, 1, 2, 4, or 16 for m equal to any of the five most frequent plaintext letters {^ E T O A}, ensuring that none of them will be encrypted into one of the five length-1 ciphertext unigrams.

8.8. Source code implementing the encryption and decryption algorithms, written in ANS standard Forth, is available on request from the author.

9. References

1. A. Dhavare, R. M. Low, M. Stamp, Efficient cryptanalysis of homophonic substitution ciphers, *Cryptologia* **37** (2013) 250-281.
2. R. Merkle, M. Hellman, On the security of multiple encryption, *CACM* **24** (1981) 465-467.
3. A. G. Reinhold, How do I use dice to create random character strings?(1995), available at http://world.std.com/%7Ereinhold/dicewarefaq.html#randomstrings.
4. R. L. Rivest, A. T. Sherman, Randomized encryption techniques, in *Advances in Cryptology: Proceedings of Crypto 82* (1982).

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

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

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

10. Appendix

C_1

```
WIJXP I-CS, XJW?Z DF.EQ MYZMP ARGPH ,XWO? HONKS PIZWH YRTGL HMOLB DAR-G UNPCR
OBLMA XYJQV EXOGL MZJD? HAYJD KTBW, NYXBL ,?OMZ PIZJP ,LBTF EQVI? KURGY MZSVF
USRKJ ABHWH NPUIA RLHGT RDKJY HNZIP .VEQT CMJIC S-BTW ,TRBP -GHWR W,ZOH NFEVH
MKC-S CF.EJ HSKRG KS-C, TBSJ- MD,.X KRDEZ DRO.X AKWE? NTFAC PAEY? DCZX? JDOBR
.JLHA XVM?. GVIBH OAZ-. KFLNT .-KQ- EYCQK VS,XO ,EBGI HYEBX .Q?ES UXI?A ZBFGK
IAPCT FNP.Y XPA,R .OYQF EKHXV GPALH XSB,T .IALR ,XWC- PIUZG HW-KJ SGRTV .QJOC
OABT? MZOXM CQFLG A,LS- BHAK- CNDKT GRSTP IZRXM J?XR- L?DSB N-XMA YXW-O MXABT
LEFQP ,TPFQ M,CIW X,MZW G-HKJ OXLHT ,AP-S BSW,U .QULD BMZLR TGJXA JDS-C DPNC.
QE-,O PHKS. FVEMG WRGTB ,YJKD PULPB ,LXCR A-HTR GIPDA HB,W- SC.VF EKR-X ,IPJR
-,LZP GTR-C AXRMN UHW?D JOHGA ,LZMP -AHBF Q.Y-L X?MAN CKL,B Y?DPM OBHA. QEOCG
OGYUR XHLWH B,TLP DHA,S NOHWA HIPUZ TGOHW NHABD NPUIW O,BTS WXAHB RXJ-L OHWUP
KY,SR TGNPI UDKAX MV.EW CILWG KNWHO LDAXY SKXW, -RF.Q LCHM, LSK,B TD?OW UG-RB
AQE.- U,LXT S,OLM HOWEQ F.Z-M AURGX CA,XW AHGTZ MJ-BL H-ACH BEF.Q JOXBH -SBL,
RXCMW IXJRQ .SGZ- XHTN- CKFEK ILIJD PWJH- AHBVE .R?BH OMYXH LAMIP ZJ?YQ EVLUA
?JTRD AWHGL HIZRA MHXLU GDPXS BW,XA XC.Q? CHJN- WIXGT RLOMY LHDAO WNX,X WYB?K
SQ.PX UJCAJ .EQGK G-L?Z S-CUY FVETM JAYTG EYWKR CNCSK YKISB JPLGA -LC.E QDIMK
ZLXOW HPINB ,SC-S YUAPL T?DJN XYH?D JIJF. WZKB, DH.FL AY,HG WX,GR YLBRT ,PJLD
KBML? FQRI? GO,WL MQ.FV YITIH -ZOJP UGRYX HDHPA RYB-H XIJ.Q VJG-A HBIJO ZAMX-
RIPZG UHGYU E.PKW SMRYF .GCUX -CYCS -BHDR YWAHB JWIXA MXNLX YDPWI S-CQ. FVX?T
COWUR WG,BU IRTBT ,SYRB N-UQV .DMGW XZPIR BCMEF .,NUN ,KJYO HWAXR C,BHW OQE.V
DSYZU ZM?LU NOZ-C SPOZA UY.FQ GAXRD J?URT JRWOL HXM?S ,-SFP YWSDY SC-XR LMHOW
PJIX, JDAXL HADJ- LMAXY JH,XT RGEVF .QUAT GUKND BCA,I JMXAT RY-SZ IHWO? ZNIS,
PGHDP B?DJH AXRS- COBL- CW,XU ZLMRJ SLT,- WS-UZ ,XWGY RUNIW X,RGA DHBLO PJLGY
PDAHC AP-AX RC-NB SRACX JRLOG WYJDK LPJCK BA.EH SGWCS -JYDK ,SPIZ K-SW, KYMLX
W,NLC SLOTG SJ,IL PJTYG HMOD? JHPAD XAMJ? KY-RK DL,BE .VQBN WAJI, XJBRV FODJR
BLKSL OMDAV FQR?T -M?HC -RTGV ,?N?O YURGM Z,LB- ROWHF .VEQZ BWZ?X WQ.FE YC,LI
JX,YR WIX-C GRYTK JYDCS LYDK, LB?LX MYX?Z MLXCV .LKMC -SGOL OMNZY RINHX YNIPH
YNX?M INC-S QEF.H SMSNR UPR-J IXMAQ EV.LU JUYGR TC-H- WGDHL HCAWX ,HOGL HMLZT
,CSLB XMA-J RPBL, GPL?Z J?Q.F COHIX HOTY? JDMOA DGRT- HIUNZ Q-YXR YGUHG V.,KH
GJ,IC S-VIY M?KNU ROGXL HE.FA ,-UOH MLZ?Y KP-MX ATUJY CXN-X IWJBD LPZIH BLRAM
XOMT, QFEAK ,OJ,L OMGYT .VFEI SUP-S FVE.Z RTC-S DPRTG NLIJP ILB,Y HXNIN -CSBD
NXHYC AOBOZ M?P-S -XNYD ?JXNH WH-D? JWJNU Q.VN? URX,K ZIPFE Q.SZD ?AHYX LNSTN
-CKMZ
(2085 characters)
```

C_2

```
D,IJT MRUWA PI,.Q -JHQW P.IZH DYA-Q UMIXG ?KISA ,NWVY CKBHU VXDJ- QZ,XV LYAGR
XMQL- XNAUJ YOMXC E-UJM X,WUD RIYFJ V.ST, MRTUM XIWGB UQXLZ -XRM. BD-,Q -DARO
GIX,I .-RGW GXHZN .WASA UW.BV NWA.R -G,VX WHSNE KMAPX DQAG- FKJRO RGO-X MULBF
.ORVS NA-DW H?IAQ NYJG- AF-NP NHYWM A.UWH ZDYGP QX,R. ODRGB HLTNA GKZCW UMOZA
-R,.U DZ?MF TLJHS GRX.P M?MXI YE?WE .KMAS DRDH- ?BGVW A?FLN T.-KQ ?QYFJ .UKED
DVRSG .QCVY GWS-Z NT.UG DCZDB -OAZF GKIAP Z-TRM .-DPT IRDYO J.USP QGZHY .-DNT
BSU.I XGWOL YHZWI DRSPI GBXSN TVRGA O.,C? KFWLD U,ITN RAGBO YJ,I? CTYWV SNJOY
D.-QB JDMRI UXARG OI.PZ WYHEC HBWJP I,QH. D-YJB ODZGX WSNTK ,AUWO YLSPG HTV,X
VHZYG WI,XV MDRTI QMUVH QIUAX ,VZFR QID.I PZWBT V?KEQ YTX-V P,Q-B NVYOJ E?KFC
HABDJ GXVNI BWGRD MBOLJ HZY-Z ,LMXD IMRTG HPKCI UNZOY LDHYZ QG.HZ QPSHM DARGQ
MULJ, IGHP, X-TBV QGZH. ,PCKN DVIOA G-RUM QL-D. NSVBK CBPWS OBIJ, LOYJX BGLYD
.-OYB JXMLG HPRTD IXIMD RPGHD WZHP, .LOBJ ANUHQ GNVTS DQSNT A.NUW GWXZX -F?EX
OY.PC K?E,G UJPJG -NTBV ZXWIO YJFK? CYSDN A.JIP MIP., SNTXW ,P.-R G.UNO LEKSY
RIQXL Z,-GO A-B.- QYL-D .NBTS X,SNV PHGJG XBFK? RXYXM WHZ,X -VTSN O-RWZ YDHF?
CUOPS AGRQH KFHBG .PIJW IGXJN .BT,A UZXV, MQUPJ ,ITRM DVX-, WBXAW .XLQM Z-AGD
IRVGQ AUP., MQX-Q DUWQD F?EHX WTBVS IMRDW UNGRA HSGPI ,ECGN YPROP LOIJ, .ZXGI
WSNBT LBJTN SLPHG Q,QXA -ORDR IOJLB -ZV,M LQUOL YHZV, Z-IKC AT,YO LXMZH .PIGW
IBMXL HGPUA N.WBT VF?EH LRLXS TNVZI WGZHD YXGSV B-Z,N V?FCD J-TWI PI.JA W.UB?
KFDUN TSVGS PHNGW XIAWU QMUWI XEFC. SVI,. WGITR ID?EP YRT-R UQXNT SPIJ. ,YDZ-
ARGZK F?CLV LJNSV OJYLE ?KWPJ UQBLY ,-ZLJ .RMT- XVHWZ KF?EW SUA,P GARWU -V,AU
WDRUX QJOYB U.NQG RGAQB .N.UW API.- XV,ST NPJ,. BXIZ- X,.B- RIDSQ GHO-R TGASV
BUMQA U?CEL HGOR- NUWAD -.FEO IOYL, P.GPH EKJX. UVNSR BE-NX VQYOL D.Q-P I,JFE
KZI-N RAHZR GAOD- ?MHLM XULI. PRAOJ DQ,MN SUWAI .HDWN .WAQP RMDUQ MHDWY CFZTW
B-R.Z ,-XTM RGRAQ XLMU, V-XMQ XVNSL UQM.W APQSW DZHYF KCLV- QMUHX MLZYH K?CFZ
QADJO VNSLO YJSVE ?FGZT ,VIZW FKCEN JN.Y. WA-QB DLMQX WXJYO ZDYHU ARGAQ D-ZMP
.I,SP QGXQM ?-PWB QUXHD WLBJZ DWYHO JY-B. QLQXN TB,.P GPHQU W,RTI DHQSW .IDRJ
X-HGP BLOJN STUWN AXV,Y OJLGW YHZIR D.,-Q D?EHI -WY,P JSZDH Q-DRM TARGM VXZRA
G.,PD ZYHLY QDBOJ YVOL- OGVSN HWZDM DW.AN MLXQG -XLQI UA,JI .DTRJ YOTBS NIMP.
,GIWE WROYX LMO-G XZ-FE RBW-G RAP,E ?CUSI QH,QD HPGSW UGARL SNVYO IZ-X. JIDQ-
CKPNW G-OW. AGPHS TVDHY ZTRDI K?FDX -MUQV X-?FC UOG,G ARO-B WIXGJ KCESO ZWXQM
THG.- DBZVX IDRUX Q,PR- BQ.-H Z.-Q? ECFOU H,HGU QXHYZ .D-JY BO.UQ GH.D- SPD-S
VNIMR TXWNC FAZBU TISVT NZHWL YAW., XVGOA R-FYM -JIDH WRDIM P.,LO JBGSQ ?MPWX
.SV?C KEGJD .BNTV RAIDR QMU-D .ZX,. ,ITNS I.PVN ECKRZ IYLBZ XFKM- IRYZH DXQGR
ATVSI M.P,H ZWI.J UWAQH GPZV- IDRYB OJQ.M DRHPG TBZ,- XP-GX GIE?F KC,YO XUQPH
GTMIH YWDZ. WATIJ BLO.P JIQMX JLIHZ P.ITB -ZB-. QRMIZ WH
(2257 characters)
```