A method for solving HEADLINE PUZZLES - by Dave Smith

INTRODUCTION

Paul Derthick developed the Headline Puzzle in the 1960's as lunchtime entertainment for people who liked to solve cryptograms.

Each Headline Puzzle contains five headlines from recent daily newspapers. Each of the five is a different monoalphabetic substitution, and all five are derived from the same mixed alphabet at different settings against itself. A complete solution includes recovering the plaintext of each HEADLINE and three key words, the SETTING, the KEY and the HAT.

In Paul Derthick's words, "The use of headlines was a happily malicious thought. It permits the inclusion of outrageous proper names, and has the tendency to exclude the commonest words." Anyone who solves cryptograms will tell you that those characteristics make them tough to decipher. But even though the five headlines may include some tough analytical problems, finding the SETTING, KEY and HAT can be even more challenging.

WALKING THROUGH A SOLUTION of a Headline Puzzle

The following Headline Puzzle was originally published in April 1996 by Larry Gray:

```
1. AMHXZLX ALXNSTXO APYBX NLJXHXK LI ZJL AHWHMHBX BHUAUBIZ;
2. GHDMRJGB MCGHE CKXCDMCQH SP RLCEE OSEE, ZHMCGHE MSU DJCC EOSM;
3. WYNAJSM PYXMKANWAJKANB VNYLXPA MAFN-VANWAPK CXMLNAL LYQQFN IJQQB;
4. XOAJRH DOHU XFNIRA MPS GRNC RBQTSPBIRBHNF FNG RBMPSDRIRBH;
5. FRHRXIQ ALVTURXF RQX. VALPPF SI VXCMRLP XLVJ LPFPVLXU
```

The general method of solution is to:

1) Decipher at least two headlines;
2) Find a mixed alphabet that deciphers all five headlines;
3) Recover the SETTING and the Index letter;
4) Recover the KEY block;
5) Recover the original mixed alphabet;
6) Finally, recover the HAT.

These general statements may seem confusing at first, but will become clearer as the method unfolds.

Step 1: **DECIPHER AT LEAST TWO HEADLINES**

Since the initial step is to solve at least two headlines, look for nice wedges in any two. Two apparent wedges in this example are the long pattern words in headlines 3 and 4. The 14 letter word in headline 3 has the pattern ABCDEFGHFIEFGJ, yielding "counterfeiters" from the pattern word dictionary. Substituting these letters in the headline produces several incomplete words (shown below). A little trial and error produces the full plaintext, "Foreign counterfeiters produce near-perfect hundred dollar bills":

```
   forei n counterfeiters  ro uce ne r- erfect  un re    o    r    i  s
3. WYNAJSM PYXMKANWAJKANB VNYLXPA MAFN-VANWAPK CXMLNAL LYQQFN  IJQQB
           ABCDEFGHFIEFGJ
```

The 13 letter pattern word in headline 4 has the pattern ABCDEFBGABHIJ, yielding "environmental" from the pattern word dictionary. Substituting the letters in the headline also produces several incomplete words; not

```
as nice, but good enough to produce "Budget cuts blamed for weak
environmental law enforcement":

       et    t    lame    or    ea    environmental  la  en or ement
4. XOAJRH  DOHU  XFNIRA  MPS  GRNC  RBQTSPBIRBHNF  FNG RBMPSDRIRBH
                                     ABCDEFBGABHIJ
```

```
Solving the first two headlines is seldom this easy; but as you can
see, long pattern words are a big help when they are available.
Otherwise, use the standard techniques of counting frequencies of
letters, digrams etc. to get started solving headlines as
monoalphabetic cryptograms, with word divisions.

The recovery of plaintext to ciphertext letters this far is:


   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
1.
2.
3. F I P L A W S C J     Q   M Y V   N B K X
4. N X D A R M J   T   C F I B P     S U H O Q G
5.
```

Figure 1

Step 2: FIND **A MIXED ALPHABET THAT DECIPHERS ALL FIVE HEADLINES**

The columns in Figure 1 are arranged alphabetically by the plaintext letters for ease in building chains. Each vertical column is fixed, regardless of the sequence of the columns because each plain letter stands for only one cipher letter in each of the headlines. The purpose of chaining is to find an alphabetic sequence for the fixed columns that is the same in each row. The sequence we derive from chaining will not necessarily be the original mixed sequence; but it will solve all five headlines when the rows are set against themselves. For the rest of this section we will refer to the mixed alphabet derived from chaining as an equivalent alphabet.

The equivalent alphabet is not unique. There are 6 equivalent alphabets which are odd decimations of the original (e.g. every third letter, every fifth letter etc. in a 26 letter cycle), 6 odd decimations that are the same as the first six, but in reverse order, 6 even decimations that give two cycles of thirteen letters each (rather than a single cycle of 26 letters), 6 even decimations that are the same as the first six even decimations, but reversed, and a single decimation with the same two letters repeated 13 times. Only the 26-letter cycles are useful results from chaining, so we will look only for odd decimations when recovering the keyblock and the original mixed alphabet. Actually, on rare occasions, an even decimation must interleave the two 13-letter cycles to get a single useful alphabet.

Chaining capitalizes on the symmetry of letter positions in the fixed columns of Figure 1 and their relative distances apart in related alphabets. For example: if plain "a" equals cipher "F" in line 3, and plain "f" equals cipher "W", then the distance between plain "a" and plain "f" is the same as the distance between cipher "F" and cipher "W" in their respective alphabets. A two-dimensional chain combines the relationships of the plain alphabet and two different cipher alphabets. In this example, we put line 3 ciphertext letters vertically under the plaintext letters; and put line 4 ciphertext letters horizontally to the right of the plaintext letters. In that way we generate a two-dimensional interactive chain with the same equivalent alphabet in each vertical line, and a different equivalent alphabet in each horizontal line. Refer to Figures 2 and 3 for what the display looks like on graph paper.

Arbitrarily starting with the plain A and cipher F (line 3) gives part of the vertical chain (A over F). Then looking at plain F over cipher W adds W to the chain (under the F). Looking at plain W, however, shows that no cipher letter has been identified in line 3 for plain W, so we show "." as a place-filler. Returning to cipher A (line 3), we find cipher A under plain E, but no cipher E to continue the chain, so we show "." as a place-filler. See the diagram in Figure 2 for the vertical chain fragment EAFW.

Then we make a horizontal chain on each of the letters of the vertical chain, using the plain alphabet and cipher line 4. The first horizontal line is from cipher R to the right of plain E, cipher S to the right of plain R, etc. giving the horizontal chain fragment ERSUOP. Similarly, completing the next three horizontal fragments looks like the matrix in Figure 2.

```
      .
      . E R S U O P .
. K C D A N B X .
    . L F M I T H .
      . W G J .
        .
```

Figure 2

Continuing to expand the chains shows quickly that the horizontal chain repeats with a 13 letter cycle, indicating that it is from an even decimation (and therefore not useful at this time). The vertical chain, however, contains a full 26 letter mixed alphabet, indicating a useful decimation. The result looks like the matrix in Figure 3 after only a few iterations.

Note how the chain fragments grow interactively, with the horizontal chain providing letters for the vertical chain and visa versa. Also note that all the vertical segments are parts of the same equivalent alphabet. When an overlap is discovered, the chain can be expanded by inspection. Look, for example, at the bottom vertical segment NMGSBI and see how it came from combining segments from the two columns to its right. Similarly, the horizontal chain segments are, by chance, part of two independent 13 letter cycles which can be expanded to other horizontal chains by inspection.

Only one letter eluded detection by two-dimensional chaining; so it isn't hard to identify it and fill in the "Z". There is no need to activate a third dimension or decipher another headline in this example.

```
I
J
U
X
T
K
O
Y
H
C
P
V
.
D
L
```

```
    Y V Q W G J K C D A N B X Y V   (13 LETTER CYCLE)
I T H . E R S U O P L F M I T H     (13 LETTER CYCLE)
J K C D A N B X Y V
    P L F M I T H .
      Q W G J K C D A N B X
      E R S U O P
  C D A N B X Y V
        M
        G
        S
        B
        I
```

Figure 3

The equivalent alphabet in this example is:

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

Step 3: **RECOVER THE SETTING AND THE INDEX LETTER**

Any of the equivalent alphabets will solve the remainder of the headlines, so we'll use this one instead of waiting until recovery of the original alphabet. Now that we have an alphabet to slide against itself, we simply write out the alphabet on a sheet of graph paper, and write it twice on a second sheet that we slide along the first. Then we attack the unsolved headlines at their shortest (usually two letter) words. Recognizing that one of those letters will be a vowel, we simply try all the vowels on one letter until the second letter makes a good word. Then we keep that slide position and try another word to verify it. Frank Lewis observes another type wedge, in "Solving Cipher Problems"; "You would be amazed at the number of times the second word ends with S and the third is a short word such as TO."

Attacking headline 1 with the slide setting in Figure 4 shows that LI = of (verified with ZJL = two), and the whole headline reads. "Clinton condemns Cuban downing of two civilian aircraft".

```
  i j u x t k o y h c p v z d l q e a f w r n m g s b
O Y H C P V Z D L Q E A F W R N M G S B I J U X T K O Y H C . .
```

Figure 4

After applying the same technique to headlines 2 (SP = of) and 5 (SI = to), the setting for each headline is shown in Figure 5. The SETTING keyword "SHARP" shows clearly under the index letter "e". We'll need both the SETTING and the Index later.

```
   i j u x t k o y h c p v z d l q e a f w r n m g s b
   ---------------------------------------------------
1. H C P V Z D L Q E A F W R N M G S B I J U X T K O Y
2. F W R N M G S B I J U X T K O Y H C P V Z D L Q E A
3. J U X T K O Y H C P V Z D L Q E A F W R N M G S B I
4. T K O Y H C P V Z D L Q E A F W R N M G S B I J U X
5. R N M G S B I J U X T K O Y H C P V Z D L Q E A F W

    Setting = SHARP  Index = E
```

Figure 5

Note: The setting might read up the column, rather than down, or be derived from plain-text alphabets under a single cipher-text alphabet, rather than cipher-text alphabets under a single plain-text alphabet.

Step 4: **RECOVER THE KEY BLOCK**

The literature suggests examining the equivalent alphabet, looking for sequences of letters (viz: ABC). Then examine the alphabet to see if another sequence is a uniform distance from each letter (viz: L is 3 before A, M is 3 before B, O is 3 before C) and decimate by the uniform distance. That works, but it's not always obvious. So I like to force the display to show me sequences by aligning the equivalent alphabet vertically in strips. For convenience they are across the middle in alphabetic sequence (similar to the sequence of unused letters in a keyblock). Then the appropriate decimation is much more obvious. See Figure 6. Sometimes the key is in plain view. The matrix in Figure 6 has its rows and columns numbered for convenience in referring to them. In practice, only the odd decimations are necessary, but Figure 6 shows the whole equivalent alphabet vertically in each column.

Look for the KEY word and for alphabetic sequences of unused letters in the key block, horizontally in Figure 6. The highest concentrations of alphabetic sequences are in rows -6, -3, 3 and 6 indicating that a decimation of three might be a good choice. This a "goodness" test, and it usually indicates the correct decimation.

-12	k	d	g	j	t	o	v	m	l	q	w	u	p	c	r	s	x	h	z	f	e	b	y	a	n	i
-11	o	l	s	u	k	y	z	g	q	e	r	x	v	p	n	b	t	c	d	w	a	i	h	f	m	j
-10	y	q	b	x	o	h	d	s	e	a	n	t	z	v	m	i	k	p	l	r	f	j	c	w	g	u
-9	h	e	i	t	y	c	l	b	a	f	m	k	d	z	g	j	o	v	q	n	w	u	p	r	s	x
-8	c	a	j	k	h	p	q	i	f	w	g	o	l	d	s	u	y	z	e	m	r	x	v	n	b	t
-7	p	f	u	o	c	v	e	j	w	r	s	y	q	l	b	x	h	d	a	g	n	t	z	m	i	k
-6	v	w	x	y	p	z	a	u	r	n	b	h	e	q	i	t	c	l	f	s	m	k	d	g	j	o
-5	z	r	t	h	v	d	f	x	n	m	i	c	a	r	j	k	p	q	w	b	g	o	l	s	u	y
-4	d	n	k	c	z	l	w	t	m	g	j	p	f	a	u	o	v	e	r	i	s	y	q	b	x	h
-3	l	m	o	p	d	q	r	k	g	s	u	v	w	f	x	y	z	a	n	j	b	h	e	i	t	c
-2	q	g	y	v	l	e	n	o	s	b	x	z	r	w	t	h	d	f	m	u	i	c	a	j	k	p
-1	e	s	h	z	q	a	m	y	b	i	t	d	n	r	k	c	l	w	g	x	j	p	f	u	o	v
Ref	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
1	f	i	p	l	a	w	s	c	j	u	o	q	g	m	y	v	e	n	b	k	x	z	r	t	h	d
2	w	j	v	q	f	r	b	p	u	x	y	e	s	g	h	z	a	m	i	o	t	d	n	k	c	l
3	r	u	z	e	w	n	i	v	x	t	h	a	b	s	c	d	f	g	j	y	k	l	m	o	p	q
4	n	x	d	a	r	m	j	z	t	k	c	f	i	b	p	l	w	s	u	h	o	q	g	y	v	e
5	m	t	l	f	n	g	u	d	k	o	p	w	j	i	v	q	r	b	x	c	y	e	s	h	z	a
6	g	k	q	w	m	s	x	l	o	y	v	r	u	j	z	e	n	i	t	p	h	a	b	c	d	f
7	s	o	e	r	g	b	t	q	y	h	z	n	x	u	d	a	m	j	k	v	c	f	i	p	l	w
8	b	y	a	n	s	i	k	e	h	c	d	m	t	x	l	f	g	u	o	z	p	w	j	v	q	r
9	i	h	f	m	b	j	o	a	c	p	l	g	k	t	q	w	s	x	y	d	v	r	u	z	e	n
10	j	c	w	g	i	u	y	f	p	v	q	s	o	k	e	r	b	t	h	l	z	n	x	d	a	m
11	u	p	r	s	j	x	h	w	v	z	e	b	y	o	a	n	i	k	c	q	d	m	t	l	f	g
12	x	v	n	b	u	t	c	r	z	d	a	i	h	y	f	m	j	o	p	e	l	g	k	q	w	s
13	t	z	m	i	x	k	p	n	d	l	f	j	c	h	w	g	u	y	v	a	q	s	o	e	r	b
	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

Figure 6

Note in column 1, for example, that the alphabetic sequence reading up the column from the reference line to -3 and -6 is ALV, and in column 2 it is BMW, and in column 3 it is COX (all in alphabetic sequence). So the apparent order of the key block is UP the columns. Since we wrote the equivalent alphabets down the columns, the decimation must be in the opposite (minus) direction. Figure 7 shows the likely keyblock lines arranging from top to bottom for ease in reading.

In forming the keyblock, the columns must stay intact to maintain the integrity of the mixed alphabet, but the rows can be rearranged because the horizontal alphabetic sequence was artificially created to get a sense of order. The key word will be on the top line of the keyblock, perhaps wrapped around onto the second line.

```
  3 r u z e w n i v x t h a b s c d f g j y k l m o p q
Ref 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
 -3 l m o p d q r k g s u v w f x y z a n j b h e i t c
 -6 v w x y p z a u r n b h e q i t c l f s m k d g j o

    1 2 3 4 5 6 7 8 9 1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
```

Figure 7

Figure 8 shows the result of developing the keyblock from the information in Figure 7. Look at line -3 in Figure 7 and strike through the columns that were not in alphabetical sequence (columns 5, 8, 9, 14, 20, 21, 22, 23, 24, and 26). Then look at what remains in row 3, and see the word "zenith". Notice that the letter C was in the reference row under the Z in zenith, so terminate the first row at B. The resulting perfect keyblock confirms the decimation of minus three.

```
z e n i t h a b
c d f g j k l m
o p q r s u v w
x y

KEY =ZENITH
```

Figure 8

Step 5: **RECOVER THE ORIGINAL MIXED ALPHABET**

The original alphabet in Figure 9 can now be read directly from Figure 6 by starting with the Index letter "e" and reading every third letter vertically in any column:

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

Figure 9

Step 6: **RECOVER THE HAT**

Two essential elements are needed to recover the hat, the transposition sequence of reading columns from the keyblock, and the relationship between the words used for the SETTING, the KEY and the HAT. The transposition sequence is the alphabetic sequence of letters in the HAT keyword. The relationship of the HAT to the SETTING and the KEY comes from a determination of the relationship between the SETTING and the KEY alone. The transposition sequence from the keyblock to the mixed alphabet can be read directly. From the original mixed alphabet in Figure 9, refer to the keyblock in Figure 8. Start with the index letter "E", read down EDPY, then down TJS, then down NFQ etc. The full sequence is shown in Figure 10.

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

Figure 10

The alphabetic sequence of letters in the hat word is 4 1 3 5 2 7 6 8; and the word is related to the KEY word (ZENITH) and to the SETTING word (SHARP).

There are at least two ways to find the hat. The method illustrated in Figure 11 uses the alphabetic sequence of each letter position in the HAT and defines the limits for each position. In the first text line of Figure 11 the letter A could be at positions 1 and 2, but not at the other position. Only position 3 could have a letter as low as B, positions 4, 5 and 7 could have letters as low as C, depending on the letter in position, positions 7 and 8 could have letters as low as D, depending on the values above. Likewise at the high end, only positions 7 and 8 could have a letter as high as Z etc.

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

Figure 11

Research on the relationships (perhaps with Google) usually recovers the hat faster and with more enjoyment than working the positional possibilities. Relating the words SHARP and ZENITH suggests manufacturers of electronic stuff like computers and radios and television sets. By examining the names of other manufacturers, like Toshiba, Panasonic, Motorola, Magnavox, Pioneer, Hitachi etc. only MAGNAVOX matches the length and alphabetic sequence. The name "HAT" appears to have come from the position of the transcription word on top of the keyblock.

```
   M A G N A V O X        Hat = MAGNAVOX
    4 1 3 5 2 7 6 8
    Z E N I T H A B        Key = ZENITH
    C D F G J K L M
    O P Q R S U V M        Setting =SHARP
    X Y

   e d p y t j s n f q z c o x i g r a l v h k u b m w
   ---------------------------------------------------
1. S N F Q Z C O X I G R A L V H K U B M W E D P Y T J
2. H K U B M W E D P Y T J S N F Q Z C O X I G R A L V
3. A L V H K U B M W E D P Y T J S N F Q Z C O X I G R
4. R A L V H K U B M W E D P Y T J S N F Q Z C O X I G
5. P Y T J S N F Q Z C O X I G R A L V H K U B M W E D
```

Figure 12

It's interesting to confirm that the original mixed alphabet in Figure 12 gives the same solution to the headlines as the equivalent alphabet developed earlier in Figure 5.

Complete Solution:

1. CLINTON CONDEMNS CUBAN DOWNING OF TWO CIVILIAN AIRCRAFT;

2. KENTUCKY TAKES ADVANTAGE OF UMASS LOSS, RETAKES TOP NCAA SLOT;

3. FOREIGN COUNTERFEITERS PRODUCE NEAR-PERFECT HUNDRED DOLLAR BILLS;

4. BUDGET CUTS BLAMED FOR WEAK ENVIRONMENTAL LAW ENFORCEMENT;

5. SILICON GRAPHICS INC. AGREES TO ACQUIRE CRAY RESEARCH

Setting = SHARP   Key = ZENITH   Hat = MAGNAVOX