SO YOU WANT TO DO THE HEADLINE PUZZLE?

Version 2.0

Author:
Bob Bogart, S31423

July 2011

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE

Table of Contents

1. History

The Headline Puzzle was a creation by NSA Research Analyst Paul Derthick, and first appeared in the November 1964 NSA Newsletter, a 16-page monthly publication produced for NSA employees. For the first few months the Headline Puzzle took turns with a crossword puzzle in the Newsletter, but in April 1965 it became a regular feature.

Mr. Derthick retired from the Agency in 1970, but continued to create the puzzle and submit it to the NSA Newsletter for publication throughout his retirement. In March 1992, health issues forced Mr. Derthick to give up composition of the Headline Puzzle, but the puzzle continued under the editorship of Larry Gray, an NSA Cryptanalyst who was a longtime friend of Mr. Derthick's since his childhood.

Mr. Derthick died in August 1998, but his brainchild lived on through Larry Gray even after the NSA Newsletter ceased publishing in October 2000. While the Newsletter may have died then, the Headline Puzzle continued, appearing in a new publication called The Communicator. In December 2002, it too ceased publication as the Agency migrated to an Intranet "publication" called NSA Daily to keep its employees informed of news and events.

After a several month hiatus, the Headline Puzzle was reincarnated in April 2003 on a monthly basis on the NSA Daily web site under the new editorship of Bob Bogart (that's me!), a Cryptanalyst who has been a Headline Puzzle junkie since coming to NSA in June 1985. More recently, the Headline Puzzle has begun appearing on its own Wiki page, which displays the current puzzle and links to past puzzles and solutions. Links also exist from the site to helpful English word pattern lists.

2. Construction of the Headline Puzzle

Before we show you how you can solve the headline puzzle, it's important to know all the pieces that go into the puzzle. First, obviously, are the headlines themselves. Five newspaper headlines are selected each month. Since I've been creating the puzzle, I've selected one headline each month from these categories: International, National, Local, Sports and Business. The headlines don't necessarily appear in that order though. The sports headline, for example, is just as likely to appear first as it is third.

There are three other parts to the equation though, and they are the **setting**, the **key**, and the **hat**. These are three words or phrases which are all "related" somehow, and working back to obtain these three ingredients is part of the Headline Puzzle solution process as well. If you can get all three, which ultimately is the goal, you'll distinguish yourself as a true Headline Puzzle aficionado.

There are some rules that are followed when choosing these three puzzle pieces:

1) The **setting** is always a five-letter word (or phrase), and letters may or may not be repeated in the setting.

2) The **key** is a word (or phrase) of any length which is somehow related to the setting. Traditionally this word has no repeated letters, but that's an "unwritten" rule that Paul Derthick, Larry Gray and I have obeyed faithfully. The reason we choose a key without repeated letters is to try to avoid any confusion over what the key word or phrase is.

3) The **hat** is a word of any length which is also somehow related to both the setting and key. Again, traditionally we choose the length of the hat to be seven letters or longer, and Larry Gray even took that a step further and tried to limit its length at 12. I've had one that was 13-long since I started (the December 2003 puzzle), but most of the time I'm following the rules that Larry used as well. Choosing a hat of length greater than 13 makes solving the puzzle much more difficult (as you'll see). Similarly, selecting a length less than seven allows for too many words to (perhaps) be included as possible solutions; again, you'll see why that is very soon.

So let's show you how I'd make a puzzle by walking you through the steps I follow when creating the puzzles. Here's how I created the March 2004 puzzle. First, I selected the headlines, one from each of my five categories. I picked these:

1. FAIRFAX APPROVES TAX PLAN FOR METRORAIL EXTENSION

2. PFIZER ENDS SALES TO CANADIAN INTERNET PHARMACIES

3. BRUNELL ON HIS WAY TO JOINING REDSKINS

4. AMID POLITICAL CRISIS, HAITIANS STRUGGLE TO FIND CLEAN WATER

5. CALIF. SENATE LEADER SEEKS BAN ON FOIE GRAS

Some hints on how I select my headlines are included in the last section of this help guide, so you can see why I chose these.

Next, I picked three words which are all related; these will become my setting, key and hat. I selected VAGUE, NEUTRAL and NONCOMMITTAL respectively.

Now I take my key, which is NEUTRAL in this instance, and create a keyword-mixed sequence based on it. A keyword-mixed sequence is created by writing down the letters in the keyword (NEUTRAL) and then following immediately with all the letters that didn't appear in the keyword in alphabetical order. So a keyword-mixed sequence based on NEUTRAL would be:

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

The next step is to scramble the letters in this sequence by placing them into a transposition matrix, and extracting letters according to the numeric key of the hat.

Say what?

Let's show you. First, how many letters long is the hat? The hat is NONCOMMITTAL, which is 12 letters long. So let's write the keyword-mixed sequence into a 12-wide matrix:

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

Next, let's place our hat atop this matrix,

```
N  O  N  C  O  M  M  I  T  T  A  L

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

and create a numeric key from NONCOMMITTAL. A numeric key is created by numbering the letters in alphabetic order from left to right. The first letter alphabetically in NONCOMMITTAL is A, so we write a "1" beneath the A:

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

C is next alphabetically, so we put a "2" under it:

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

I and L are next, so they get a "3" and "4" respectively:

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

M is next alphabetically, and we have two of them, so we enumerate them with "5" and "6" going from left to right:

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

Continuing, the N's get "7" and "8", the O's receive "9" and "10", and the T's are assigned "11" and "12":

```
N  O  N  C  O  M  M  I  T  T  A  L
7  9  8  2 10  5  6  3 11 12  1  4
-------------------------------
N  E  U  T  R  A  L  B  C  D  F  G
H  I  J  K  M  O  P  Q  S  V  W  X
Y  Z
```

And we're done creating the numeric key. So the numeric key for NONCOMMITTAL is `7 9 8 2 10 5 6 3 11 12 1 4.`

We now use this numeric key to extract columns from the matrix, forming a 26-long sequence of letters. Appearing beneath the column with "1" at the top are the letters F and W. They will form the beginning of our 26-long sequence of letters:

```
F W...
```

Under the "2" are the letters T and K. We add them to our sequence:

```
F W T K...
```

In the column with a "3" on top we find B and Q, so we include those next in the sequence:

```
F W T K B Q...
```

And continuing in this fashion, and extracting the letters in the remaining columns according to the order provided by NONCOMMITTAL's numeric key, we get:

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

Alright, so what have we done so far? We created a keyword-mixed sequence based on the key, and wrote it into a matrix which was the width of the hat's length. We then used a numeric key based on the hat to pull columns from this matrix, forming a 26-long sequence.

This sequence of letters will now be used to encipher each of the five headlines. Now, there's one piece that we haven't used yet, and that's the setting. This will tell us how to align our 26-long sequence against itself to encipher each headline.

Our setting this time is VAGUE. The setting determines how our 26-long sequence will be matched up against itself to encipher the headlines, and appears beneath the first letter of the plain component. Huh? Let's show you. We take the 26-long sequence that we created above and use it as the top line in a matrix. Then we re-write the same sequence five times, but offset it according to the setting:

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

See, it's the same 26-long sequence, except we "shove it over" so that we have the setting (VAGUE in this case) reading down beneath the first letter.

We then use this matrix to encipher each of the headlines we had previously selected. Using the top line of the matrix as the plaintext values, the line immediately beneath it (the one starting with "V") will be the alignment of the cipher values for the first headline. Let's show you.

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

With the top line representing the plaintext, and the line beneath it representing the cipher values for the first headline, we can now encipher the first headline:

1. FAIRFAX APPROVES TAX PLAN FOR METRORAIL EXTENSION
1. VXEZVXG XLLZADJC WXG LOXP VAZ RJWZAZXEO JGWJPCEAP

We now take the top line of the matrix and use it again to represent the plaintext values, but this time pull off the second line within the matrix (the one beginning with "A") and encipher the second headline:

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

2. PFIZER ENDS SALES TO CANADIAN INTERNET PHARMACIES
2. ZAFWVT VRGQ QJIVQ LE BJRJGFJR FRLVTRVL ZMJTKJBFVQ

Repeating the same procedure, we use the top line and the third line within the matrix (the one starting with "G") to encipher Headline Number 3:

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

3. BRUNELL ON HIS WAY TO JOINING REDSKINS
3. LFMISJJ UI ZDK XYR AU CUDIDIN FSBKODIK

We'll use the top line and fourth line of the matrix to encipher the fourth headline:

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

4. AMID POLITICAL CRISIS, HAITIANS STRUGGLE TO FIND CLEAN WATER
4. SLXH FDVXEXPSV POXNXN, TSXEXSWN NEOBMMVG ED UXWH PVGSW JSEGO

And finally, we'll encipher the fifth headline using the top line of the matrix for plain, and the bottom line for cipher:

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

5. CALIF. SENATE LEADER SEEKS BAN ON FOIE GRAS
5. HVWOE. YAKVZA WAVUAP YAARY MVK FK EFOA SPVY

This gives us the five enciphered headlines used in the March 2004 puzzle:

1. VXEZVXG XLLZADJC WXG LOXP VAZ RJWZAZXEO JGWJPCEAP

2. ZAFWVT VRGQ QJIVQ LE BJRJGFJR FRLVTRVL ZMJTKJBFVQ

3. LFMISJJ UI ZDK XYR AU CUDIDIN FSBKODIK

4. SLXH FDVXEXPSV POXNXN, TSXEXSWN NEOBMMVG ED UXWH PVGSW JSEGO

5. HVWOE. YAKVZA WAVUAP YAARY MVK FK EFOA SPVY

3. Solving the Headline Puzzle

For demonstration purposes, let's solve the July 2005 Headline Puzzle, to give you an idea of how one might begin the puzzle, and we'll carry it right on through to recover the setting, key and hat as well.

Here's the July 2005 Headline Puzzle:

1. BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH

2. BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS

3. ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

4. GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

5. KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW

Where does one begin? Well, there are several ways to start. Some people count the number of times each cipher letter appears in a headline, and then try to match frequently used letters in English to those frequently used cipher letters. That's not necessarily a bad thing to try, but with the Headline Puzzle it may not be the best. The headlines selected tend to be short, which will make the frequency counts unreliable.

A better way to start might be by trying to recognize word patterns. Any cipher word which contains at least one repeated letter has a pattern, and that pattern can be searched for in an English word pattern listing. What's that? You don't have an English word pattern list? Send an e-mail to me, Bob Bogart, and I'll happily send one to you.

Let's talk about patterns a bit. Word patterns are created by locating the first repeated letter in a word, and the last repeated letter in a word, and using the span of letters between them to create the pattern. For instance, let's take the English word CONFIDENTIAL and determine its word pattern. Looking from left to right, the first repeated letter in CONFIDENTIAL is N; there are two of them in the word. Now looking from right to left, the last repeated letter in CONFIDENTIAL is I; there are also two of them. Our word pattern will begin with the first N in CONFIDENTIAL, and continue through the last I in the word. Let's demonstrate.

All occurrences of the first repeated letter are labelled "A". So in our word CONFIDENTIAL. the first repeated letter is N, so label all Ns with an A:

```
C O N F I D E N T I A L
    A         A
```

Now, moving from left to right, the next letter after the first N in CONFIDENTIAL is F. Assign it and any other F's in CONFIDENTIAL the label of B. There's only the one F, so it's the only letter receiving a B label:

```
C O N F I D E N T I A L
    A B       A
```

Continuing from left to right, I is next, and it and any other I's in the word are given the label of C:

```
C O N F I D E N T I A L
    A B C     A   C
```

Next is the D in CONFIDENTIAL, it gets the label of D, and the letter E will receive E for its label:

```
C O N F I D E N T I A L
    A B C D E A   C
```

One more letter to go! Assign the T in CONFIDENTIAL the label of F, and we will have a pattern which begins with the first repeated letter in our word (N), and runs through the final repeated letter in the word (I).

```
C O N F I D E N T I A L
    A B C D E A F C
```

Thus, CONFIDENTIAL has the word pattern ABCDEAFC.

When a word in the Headline Puzzle is enciphered, its pattern will still remain the same. So, if you can find a cipher word with one or more repeated letters, you might be able to use an English word pattern list to locate potential words to fit into the puzzle.

Taking our example pattern ABCDEAFC from the word CONFIDENTIAL, we can look in a word pattern list for all the words with a pattern of ABCDEAFC. Doing so, we find these entries:

ABCDEAFC	M ACDONALD
ABCDEAFC	ADEQUATE LY
ABCDEAFC	IN ADEQUATE
ABCDEAFC	DES IGNATION
ABCDEAFC	RES IGNATION
ABCDEAFC	CO NFIDENTI AL
ABCDEAFC	V OCATIONA L
ABCDEAFC	GUBE RNATORIA L

So if we had encountered a word in the Headline Puzzle with a pattern of ABCDEAFC, any of these words would be possible decryptions of that word. But we can eliminate seven of these eight possible words! There's only one word which had two letters prior to the start of the ABCDEAFC pattern, and two letters following the conclusion of the pattern, and that is CONFIDENTIAL.

Now that you know how word patterns work, you might be able to think of common words that might match patterns appearing in the Headline Puzzle.

Looking back again at the July 2005 puzzle, are there any headlines which feature really good patterns that we might use to help us solve a headline?

1. BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH

2. BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS

3. ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

4. GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

5. KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW

Headline 4 has two words which have multiple repeated letters, GDQJBDG and BOOWZO. So let's arbitrarily start with this headline. BOOWZO has a word pattern of AABCA, with one letter appearing before the pattern. Looking in my handy-dandy English word pattern list, I find 16 words with the pattern AABCA:

```
AABCA                F EEBLE
AABCA                N EEDIE ST
AABCA                B EETLE
AABCA               SA GGING
AABCA              SLU GGING
AABCA               WA GGING
AABCA               ZI MMERM AN
AABCA                A NNOUN CE
AABCA                A NNOUN CED
AABCA                F OOTHO LD
AABCA               BA RRIER S
AABCA               CA RRIER
AABCA               CA RRIER S
AABCA                A SSETS
AABCA               RU SSIAS
AABCA                I SSUES
```

Eliminating all the words which don't have exactly one letter preceding the pattern, and no letters following it, we only have these remaining possibilities:

```
AABCA                F EEBLE
AABCA                B EETLE
AABCA                A SSETS
AABCA                I SSUES
```

We can actually eliminate B EETLE as well. Since the cipher word was BOOWZO, a plaintext B would equate to a ciphertext B if it were BEETLE, and that cannot happen in the headline puzzle, so we can remove it from consideration as well, leaving us just these three candidates:

```
AABCA                F EEBLE
AABCA                A SSETS
AABCA                I SSUES
```

Let's try them in turn to see what the headlines would look like by forcing each of these words where BOOWZO occurs:

```
     F F      EEF  L       F       F   F          F   FEEBLE  L
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

That's an awful lot of F's, and there aren't many common two-letter words which begin with F, so let's try ASSETS and see if that works any better.

```
     A A      SSA  T       A       A   A          A   ASSETS  T
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

This doesn't look too bad. Let's try ISSUES and try to determine which one seems better.

```
     I I      SSI  E       I       I   I          I   ISSUES  E
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

Hmmm, this looks pretty good as well. We do still have the GDQJBDG word which has a pattern of ABCDEBA with no letters appearing before or after the pattern. Consulting the English word pattern listing, these words have the ABCDEBA pattern:

```
ABCDEBA                    CARDIAC
ABCDEBA                    DECRIED
ABCDEBA                    DELAYED
ABCDEBA                  R ESPONSE
ABCDEBA                  D ETONATE
ABCDEBA                    INDEMNI TY
ABCDEBA                  D ISPERSI ON
ABCDEBA                    MONTGOM ERY
ABCDEBA                    NEWSMEN
ABCDEBA                    RECOVER
ABCDEBA                    RECOVER Y
ABCDEBA                ADJU STMENTS
ABCDEBA                    SURPLUS
ABCDEBA                    THOUGHT
```

Eliminating all the words with letters appearing before or after the pattern, leaves only these for consideration:

```
ABCDEBA                    CARDIAC
ABCDEBA                    DECRIED
ABCDEBA                    DELAYED
ABCDEBA                    NEWSMEN
ABCDEBA                    RECOVER
ABCDEBA                    SURPLUS
ABCDEBA                    THOUGHT
```

If ASSETS is the word which replaces BOOWZO, we'll need to have an A showing three letters from the end in the GDQJBDG word. None of these words has an A three from the end, so it's probably ISSUES that replaces BOOWZO.

If ISSUES is indeed the word that fits at BOOWZO, we'll need an I to appear in the GDQJBDG word, three letters from the end.

```
     I I      SSI  E       I       I   I           I   ISSUES  E
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

This eliminates all but these two possibilities:

```
ABCDEBA                                  CARDIAC
ABCDEBA                                  DECRIED
```

We can now eliminate DECRIED as well. If ISSUES is correct, the E in ISSUES matches with the Z in BOOWZO. With plaintext E equal to cipher Z, plaintext E cannot also equal cipher D, which it would have to do if GDQJBDG was DECRIED.

Therefore, GDQJBDG is most likely CARDIAC. Let's fill that in and maybe we can guess some more words in the headline:

```
    CI I      SSI  E   A  I  CARDIAC I   A      IR  ISSUES RECA
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

Looking great! Let's see if we can get that last word. A six-letter word that begins RECA-- and has the same letter for the fifth and sixth letter. RECALL is probably correct, so let's let the Ps be Ls and see how that affects the rest of the headline.

```
    CI I      SSI LE  LA  I  CARDIAC I  LA     IR  ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

Do you have any guesses for the second word in the headline? If not, there is a word pattern, a short one, AA, as the two Os are the only repeats in the word. Consulting the word pattern list for when the AA pattern would be SS, POSSIBLE shows up as the only possibility with I for the fifth letter, L for the seventh, and E for the 8th. Let's fill in POSSIBLE.

```
    CI I   POSSIBLE  LA  I  CARDIAC I PLA     IR  ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

How about the word after CARDIAC, any guesses there? No repeated letters, so no pattern, but maybe if you think long enough you'd come up with IMPLANT. Let's put that in and see how the headline looks now:

```
    CITIN  POSSIBLE  LA  IN CARDIAC IMPLANT   IRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

I think we're definitely on the right track. The first word looks like CITING, and the word before ISSUES appears it could be FIRM. Let's fill those in and take a gander:

```
    CITING POSSIBLE FLA  IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

The only word that hasn't been completed is the third word, FLA-. It can't be FLAG as we've already recovered a G to match cipher L, but FLAW seems like a good possibility. Filling in the W above the S, the headline reads in its entirety:

```
    CITING POSSIBLE FLAW IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP
```

Congratulations! We've completed one headline! Don't worry, we won't have to do this pattern finding technique for all the headlines, just the first couple. You can use the relationship that the plain alphabet and the cipher alphabets are identical to each other, just offset against one another, to your advantage.

In order to do that though, we first need to take the recoveries we've made and enter them into a matrix. Place the plain alphabet on top, and fill in the cipher values beneath. Because we have five headlines, and this was the fourth headline, we'll place our recoveries in a matrix that looks like this, entering values into the fourth cipher row:

```
 P:  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

C1:
C2:
C3:
C4:
C5:
```

In the word CITING, the plain C matched with the cipher G, so let's fill in a G beneath the plain C on the fourth cipher line:

```
 P:  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

C1:
C2:
C3:
C4:      G
C5:
```

Continuing on with CITING, plain I matched with cipher B, plain T with cipher Y, plain N with cipher H and plain G with cipher L. Filling in those entries, the matrix looks like:

```
    CITING POSSIBLE FLAW IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

 P:  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

C1:
C2:
C3:
C4:     G       L   B         H           Y
C5:
```

And continuing with the same technique throughout the rest of the headline, the matrix becomes:

```
 P:  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

C1:
C2:
C3:
C4:  D F G J Z E L   B     P R H K U   Q O Y W   S
C5:
```

A couple of notes here. We don't know for certain that the plaintext alphabet is in A-Z order. In fact, it's assuredly not. If it were, all the cipher alphabets would also be in A-Z order, and you can see that's not happening on the fourth cipher line. We have to start somewhere though, and putting the plain in A-Z order is a reasonable place to start.

The next technique we'll learn is called **chaining**. This will help us not only figure out the next headline we solve, but will eventually help us determine the true 26-long sequence of letters that was used for both the plain and the cipher alphabets when the headlines were enciphered.

We use chaining to take advantage of the fact that if two letters are some distance apart in the plain alphabet, they'll also be the same distance apart in the cipher alphabet. To many, chaining is like magic; they don't quite understand how it works, but they know it does indeed work and brings about some amazing results. Besides, it's fun.

Remembering that the original plain and cipher alphabets are the same, just offset some distance, we can begin by chaining a plain letter to a corresponding cipher letter. Let's start with plain A, and chain it to cipher D (in the fourth alphabet). Then, look for D in the plain alphabet and see that it matches up with J in the fourth cipher alphabet. So we have ADJ as a chain.

Again, what's this mean? It means that the distance from A to D in the original 26-letter sequence is the same distance as from D to J.

Unfortunately, we can't continue our chain any further as plaintext J doesn't have a value entered in the fourth cipher line; J wasn't used in the fourth headline.

But let's continue making chains using the plain alphabet and the recoveries on the fourth cipher line:

```
 P:  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

C1:
C2:
C3:
C4:  D F G J Z E L   B     P R H K U   Q O Y W   S
C5:
```

We already have ADJ as a chain. Let's start with the plain B and see where this leads.

Plain B matches with cipher F; plain F matches with cipher E; plain E matches with cipher Z, and the chain ends there with BFEZ. But we can also work backwards! Is there a plaintext letter that matches with cipher B on the fourth line? Yes, plain I does, making our chain IBFEZ. Nothing goes to I on the fourth line though, so this chain ends at IBFEZ.

Continuing on, we can also form these chains: CGLPUWSOK, MRQ, NH, and TY.

So we have these six chains, and we hope to eventually "link" them together to make a 26-long sequence.

In the meantime, let's tackle another headline, and use these chains to help us solve it.

```
1.  BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH


2.  BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS


3.  ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

    CITING POSSIBLE FLAW IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP


5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Why don't we try the fifth headline? It's got a nice pattern in the first word, plus there's a word with an apostrophe. Almost certainly the cipher T after the apostrophe will be an S, giving us a start on solving the headline right from the get-go. Let's fill it in...

```
              S         S    S          S        S
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Remember, I said we could use those chains we'd created to help us break into additional headlines? Here are the six chains we got when we chained the plain alphabet to the fourth headline's cipher letters:

```
ADJ IBFEZ CGLPUWSOK MRQ NH TY
```

This is cool -- you'll like this...

Since we have both T and S appearing in our chains, align the two chains involving those letters so that S is above T:

```
                    CGLPUWSOK
                          TY
```

If cipher T changes to plaintext S, then cipher Y will change to plaintext O as well (notice the Y landing beneath the O in this alignment). You can do this? Yes indeed, and again it's not important why this works. What's important is that it does work, and will give us an additional recovery in this headline.

(For those of you worrying your heads about why this works, again, since the same 26-long sequence was used for the plain and cipher alphabets, just slid at an offset, this tells us that the distance from T to S is the same as the distance from Y to O in the original sequence.)

Filling in plaintext Os where the cipher Ys appear, we get this:

```
         O   S  O     S O  S          S   OO  S
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

This looks pretty good -- there are several two-letter words that begin with an O: OF, ON, OR...

We haven't taken advantage of that nice pattern in the first word yet. KENLYKEQT has a pattern of ABCDEAB. Consulting the English word pattern book, these words have no letters prior to the pattern:

```
ABCDEAB                    INJURIN G
ABCDEAB                    INSURIN G
ABCDEAB                    INVADIN G
ABCDEAB                    NATIONA L
ABCDEAB                    REPAIRE D
ABCDEAB                    REQUIRE
ABCDEAB                    REQUIRE D
ABCDEAB                    RESTORE D
```

None of them have two letters following the pattern as KENLYKEQT does, but NATIONALS looks really good. My word pattern listing was made before the Nationals came to Washington. But this reminds me: the local sports teams are excellent words to use when breaking into the puzzles as ORIOLES, REDSKINS, TERRAPINS, and NATIONALS all have repeated letters and do show up fairly regularly in the sports headlines. Let's put NATIONALS as the first word of the fifth headline, but let's do it one letter at a time to take advantage of the chains we have from headline #4.

```
    N   ON  S  O     S ON S  N      S   OO  S N
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Here again are our chains from headline #4.

```
ADJ  IBFEZ  CGLPUWSOK  MRQ  NH  TY
```

Aligning the N and K we get this:

```
                          NH
                    CGLPUWSOK
```

Unfortunately, there is no overlap of any other letters, so we can't benefit by getting "free recoveries" anywhere else in the headline. Continuing, we can make all the E's become A's:

```
    NA  ONA S  O     S ON S  N      S   OO  S N
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

And attempting the alignment of chains trick, we see this:

```
                       ADJ
                    IBFEZ
```

So if E's change to A's, then Z's must change to D's. We add that into the headline too:

```
    NA  ONA S  O     S ON S  N  D   S   OO  S N
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

N's become T's:

```
    NAT ONA S TO     S ON S  N  D   S   OO  S N
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW

                    TY
                    NH
```

And H's become Y's -- too bad we don't have any H's in the headline.

Continuing to place NATIONALS as the first word of headline #5, L's become I's:

```
    NATIONA S TO     S ON S  N ID   S   OO  SIN
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

And if we align our chains with L beneath I, look at the overlap:

```
          IBFEZ
CGLPUWSOK
```

So if L becomes I, then P's become B's, U's become F's, W's become E's and S's become Z's. Pretty neat! Lots of free recoveries. Filling all these in, we get:

```
    NATIONA S TO  B  S ON S  NEIDE  S B OO  SIN  E
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Changing the Q's to L's to complete NATIONALS:

```
    NATIONALS TO  B  S ON S  NEIDE  S BLOO  SIN LE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Can we get any more free recoveries?

```
CGLPUWSOK
MRQ
```

Yes! M's become C's, and R's become G's:

```
    NATIONALS TO  B CS ON SC NEIDE  S BLOO  SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

All that filled in just from NATIONALS and the aligning of the chains trick. Cool stuff! Okay, where now? Looks like a BLOOP SINGLE, so let's make the As be Ps.

```
    NATIONALS TOP B CS ON SC NEIDE  S BLOOP SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Aligning chains:

```
CGLPUWSOK
  ADJ
```

D changes to U, and if we had J's they'd become W's:

```
    NATIONALS TOP BUCS ON SC NEIDE  S BLOOP SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

At this point, you have to either recognize that Brian SCHNEIDER was the Nationals player who hit the bloop single, or you can just leave the two remaining letters blank and recover them later. If we were able to recognize the player's name as SCHNEIDER, our headline reads as:

```
    NATIONALS TOP BUCS ON SCHNEIDER S BLOOP SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Just as we did with headline #4 once we'd solved it entirely, we need to fill in the recovery matrix and create more chains.

Filling in the recoveries from headline #5, the matrix looks like this:

```
 P:  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

C1:
C2:
C3:
C4:  D F G J Z E L   B     P R H K U   Q O Y W   S
C5:  E P M Z W   R X L     Q   K Y A   B T N D
```

And making chains from the plain alphabet to the fifth headline cipher values:

```
GRBPAEW  CM  UDZ  HX  ILQ  STNK  OY
```

Nicely done! We now have two headlines completely solved:

```
1.  BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH


2.  BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS


3.  ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

    CITING POSSIBLE FLAW IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

    NATIONALS TOP BUCS ON SCHNEIDER S BLOOP SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

And we have two sets of chains:

```
4. ADJ  IBFEZ  CGLPUWSOK  MRQ  NH  TY

5. GRBPAEW  CM  UDZ  HX  ILQ  STNK  OY
```

The next technique we'll learn is called **geometric chaining**, and will take the two sets of chains that we have from the fourth and fifth headlines and try to link them together to get a 26-long sequence, or at least close to a 26-long sequence. What we'll do is select a set of chains, and enter them horizontally into a grid, and use the other set of chains by entering them vertically. A good rule of thumb is start with the longest chain and enter it horizontally. Looking at our chains:

4. ADJ IBFEZ CGLPUWSOK MRQ NH TY

5. GRBPAEW CM UDZ HX ILQ STNK OY

The CGLPUWSOK chain is the longest. so let's write it horizontally:

```
C G L P U W S O K
```

Now look at the chains in the other set. If there are any letters in these chains which share common letters with the CGLPUWSOK chain, we can write them in a vertical fashion so that they intersect. For instance, GRBPAEW has several letters in common with CGLPUWSOK so we can write the GRBPAEW chain downward so it overlaps with those letters in common:

```
        G
        R
        B
    G   P
    R   A
    B   E
C G L P U W S O K
  R   A
  B   E
  P   W
  A
  E
  W
```

Here are our chains again, with the ones we've used in **bold**:

4. ADJ IBFEZ **CGLPUWSOK** MRQ NH TY

5. **GRBPAEW** CM UDZ HX ILQ STNK OY

We'll continue placing our chains into this grid with all chains in the set coming from headline #4 written horizontally, and those from #5 vertically.

Adding in the CM, UDZ, ILQ, STNK and OY chains going downward, we have:

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

4. ADJ IBFEZ **CGLPUWSOK** MRQ NH TY

5. **GRBPAEW CM UDZ** HX **ILQ STNK OY**

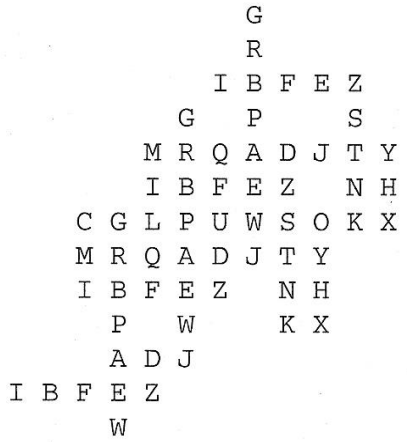
Now we can return to the fourth headline's chains and place ADJ, IBFEZ and NH horizontally. By serendipity, already MRQ and TY have appeared:

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

4. **ADJ IBFEZ CGLPUWSOK MRQ NH TY**

5. **GRBPAEW CM UDZ** HX **ILQ STNK OY**

Only the HX chain from the fifth headline remains. Let's place it into the grid:



4. **ADJ IBFEZ CGLPUWSOK MRQ NH TY**

5. **GRBPAEW CM UDZ HX ILQ STNK OY**

We haven't been able to create a 26-long string of letters yet, but we have some pretty big chunks going across this grid. Solving one more headline should get us closer. And we can use this new two-dimensional grid to speed the action along again. By guessing just one letter correctly, we should get a plethora of free recoveries. Let's show you how. Back to our headlines.

1. BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH

2. BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS

3. ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

CITING POSSIBLE FLAW IN CARDIAC IMPLANT FIRM ISSUES RECALL

4. GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

NATIONALS TOP BUCS ON SCHNEIDER S BLOOP SINGLE

5. KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW

Two letter words are a good thing to try at this point as there are a limited number of them in English. The most common two-letter words in everyday English, in descending order of frequency, are OF, TO, IN, IS, IT, AS, HE, BE, BY, ON, OR, AT, MY, AN, SO, IF, NO, WE, UP, DO, and US. So let's try to guess one letter of a two-letter word and see if we can recover a headline quickly.

What if the ZC in the second headline was a two-letter word starting with O? In the grid, if Z goes to O, you just go one space diagonally down to the right to get to O (a southeasterly direction). If Z goes to O, what does the C in ZC go to? You'd also have to go diagonally down one to the southeast to find the letter that C would change to. It's an R! If Z goes to O, then C goes to R, and we'd have the word OR!

```
                R   OR                  O R    OR     R
2.  BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS
```

If this is the case, every cipher letter in the second headline should decrypt to its correct plaintext value just by finding the cipher letter in our grid, and reading down diagonally to the southeast.

It's important to realize that when doing geometric chaining, there are several "directions" that may be equivalent. For instance, in the grid shown below, notice that you can also travel from Z to O by going up two lines and then three spaces to the right. Whatever direction works for you is fine, as long as it lets you get from the cipher letter to its corresponding plain value.

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

Let's see what happens when we take the second headline and try to decrypt as much as we can by traveling in that southeasterly fashion:

```
    UZBE  QUANDARY FOR BUSH  PUSH DE O RA Y OR SE UR TY
2.  BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS
```

Wow, just one letter guessed correctly, and it's almost all filled in. The missing words appear to be UZBEK, DEMOCRACY and SECURITY. Let's fill them in, complete the recovery matrix. and make chains from the plain to the second headline's cipher letters.

UZBEK QUANDARY FOR BUSH PUSH DEMOCRACY OR SECURITY

2. BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS

```
 P: 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

C1:
C2: L M O P Q R   T H   V   Y J Z I G C E W B       S A
C3:
C4: D F G J Z E L   B     P R H K U   Q O Y W   S
C5: E P M Z W   R X L     Q   K Y A   B T N D
```

2. FRCOZAL UBMYSEQG DPIHTW KV NJ

4. **ADJ IBFEZ CGLPUWSOK MRQ NH TY**

5. **GRBPAEW CM UDZ HX ILQ STNK OY**

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

It's easy to see the chains from the second headline should run in a northwesterly diagonal direction.

Filling them in:

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

2. **FRCOZAL UBMYSEQG DPIHTW KV NJ**

4. **ADJ IBFEZ CGLPUWSOK MRQ NH TY**

5. **GRBPAEW CM UDZ HX ILQ STNK OY**

We now try to link the lines together so they overlap and make a 26-long sequence. Start anywhere, say, with this line:

T Y C G L P U W S O K X

There's another line right below it that looks like this:

H M R Q A D J T Y C

We see the letters H M R Q A D J come immediately before T Y C, so link these two chains together to make a big chain:

H M R Q A D J T Y C G L P U W S O K X

Now using this line:

I B F E Z V N H M R

We can make an even bigger chain:

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

And that's it! We've made a 26-letter sequence!

Now, this may or may not be the actual sequence used to encipher the headlines. If it's not, it's what's called an **equivalent primary component** (or **EPC**), a sequence possessing all the same properties of the original sequence.

Now that we have a 26-long sequence, it's time to re-write our old recovery matrix with the plain and cipher alphabets in this order. Our old matrix was:

```
 P:  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

C1:
C2:  L M O P Q R   T H   V   Y J Z I G C E W B       S A
C3:
C4:  D F G J Z E L   B     P R H K U   Q O Y W   S
C5:  E P M Z W   R X L     Q   K Y A   B T N D
```

But using this new 26-long sequence we've recovered by geometric chaining, we can make the plain and cipher both be in this same order, sliding the order of the cipher until it matches the plain correctly:

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

C1:
C2:  H M R Q A D J T Y C G L P U W S O K X I B F E Z V N
C3:
C4:  B F E Z V N H M R Q A D J T Y C G L P U W S O K X I
C5:  L P U W S O K X I B F E Z V N H M R Q A D J T Y C G
```

and all of our original recoveries still hold: A in plain is L in cipher in the second headline, A in plain is D in cipher in the fourth headline, E in plain is W in cipher in the fifth headline, etc.

We still have two headlines to solve:

```
1.  BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH

    UZBEK QUANDARY FOR BUSH  PUSH DEMOCRACY OR SECURITY
2.  BAMQV GBLJPLCS RZC MBET: IBET PQYZOCLOS ZC EQOBCHWS


3.  ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS

    CITING POSSIBLE FLAW IN CARDIAC IMPLANT  FIRM ISSUES RECALL
4.  GBYBHL UKOOBFPZ EPDS BH GDQJBDG BRUPDHY, EBQR BOOWZO QZGDPP

    NATIONALS TOP BUCS ON SCHNEIDER S BLOOP SINGLE
5.  KENLYKEQT NYA PDMT YK TMXKWLZWB'T PQYYA TLKRQW
```

Let's take the first headline and see if we can figure out one of its two-letter words:

```
1.  BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH
```

This is our 26-long sequence:

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

Let's see if we can figure out what AH must be. Find the A, and H is four letters to its left. That means that if we can correctly guess the first letter of the word, four letters to the left of it is the second letter of the word. If we go one letter to the left of A we get Q, and one letter to the left of H we get N. QN is not a word, so continue.

Two letters to the left of A is R, two to the left of H is V. RV is probably not it, although abbreviations and acronyms have been used in headlines before. Keep it in mind in case we can't find anything better.

Continuing, three to the left of A is M, three to the left of H is Z. MZ, nope...

Eventually we get to 11 letters to the left of A is I, and 11 letters to the left of H is S. So let's make AH be IS, and also change every cipher letter shown in the first headline to the letter 11 to the left of it in our sequence.

```
    CRAB HARVEST IS DELAYED TO HELP MIGRATING BIRDS
1.  BUSD LSUCTHX AH OTESITO XM LTEZ PAFUSXAGF DAUOH
```

Sliding the sequence to make these recoveries true in our matrix we get:

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

C1:  A D J T Y C G L P U W S O K X I B F E Z V N H M R Q
C2:  H M R Q A D J T Y C G L P U W S O K X I B F E Z V N
C3:
C4:  B F E Z V N H M R Q A D J T Y C G L P U W S O K X I
C5:  L P U W S O K X I B F E Z V N H M R Q A D J T Y C G
```

Alright, one headline to go. Things will really speed up now...

Remember, there's a five-letter word that reads downward within the matrix, the setting, which is how the plain alphabet and the cipher alphabets align. Looking within the matrix, do you see any columns which would be good candidates for the setting's location? In other words, by filling in a letters in the third row, can you make any good five-long words reading downward?

SLIDE looks reasonable beneath the plaintext "A". Let's give it a shot.

If we align our 26-long sequence so the I from the third headline matches with the "A" in plaintext, the matrix looks like this:

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

C1:  A D J T Y C G L P U W S O K X I B F E Z V N H M R Q
C2:  H M R Q A D J T Y C G L P U W S O K X I B F E Z V N
C3:  Y C G L P U W S O K X I B F E Z V N H M R Q A D J T
C4:  B F E Z V N H M R Q A D J T Y C G L P U W S O K X I
C5:  L P U W S O K X I B F E Z V N H M R Q A D J T Y C G
```

That's nice, but until we decrypt the third headline, we won't know for sure if our guess of SLIDE is correct or not. But, when we decrypt the third headline, we get this:

```
    SHUTTLE BACK IN PLACE FOR JULY LAUNCH
3.  ASREEHL CIVJ YW MHIVL GDK FRHZ HIRWVS
```

If you didn't see SLIDE reading down, you could have still solved the headline in the same way as we did the previous two by using a two-letter word: locate the cipher Y and W in our 26-long sequence, and then move to the left or right of each of those letters the same distance to try to find a two-letter word. Sure enough: 15 to the left of Y is I, and 15 to the left of W is N, so YW deciphers to IN.

We now have the five headlines solved, and the setting, SLIDE, recovered. Next we need to recover the key and hat used.

The setting appears beneath the plaintext "A" in the matrix. This is important as it tells us what the first letter of our 26-long sequence is. So the 26-long sequence we recovered is:

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

This might be the 26-letter sequence that was used as the plain and cipher components when enciphering the headlines, but not necessarily. Remember, I said that this could also be an **equivalent primary component (EPC)**, a sequence that has all the properties of the original sequence. The sequence we have here might just be a **decimation** of the original 26-long sequence used, the sequence re-written so that the letters are just a different distance apart.

Let's demonstrate with the regular A-Z alphabet:

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

What would this sequence look like if we re-wrote it, starting with A, and then taking every third letter in turn? Start with A, count down three to D, count three more to G, etc. It would look like this:

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

And what would the A-Z sequence look like if we took every fifth letter? It would look like this:

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

We could do the same thing for other distances starting with A. These are all Equivalent Primary Components. Our sequence may very well be an EPC of the original.

We can work backwards though from an EPC to obtain the original sequence used. Look again at the sequence that was formed when we made a decimation 3 sequence from the A-Z sequence:

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

What would happen if we took this sequence and decimated it by 9? Start at the A, and count nine to the right. You land at B. And what if you continue counting, going nine to the right of B? That's right, you come to C. By continuing in this "nine to the right" fashion, we'll get back to the original A-Z sequence.

That's what we want to do with our 26-long sequence that we recovered from the headlines. Take decimations of it in an attempt to find the true sequence that was used.

So back to the sequence we recovered. Let's make decimations of it at 3, 5, 7, 9, and 11:

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

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

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

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

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

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

Okay, a couple of things here before we proceed. Why did I do only odd decimations, and not even decimations? Well, with a 26-long sequence, if I'd done a decimation of 2, I'd only get every other letter, and after 13 iterations, I'd be back to where I started, leaving half the letters untouched. And this is true for any even number. If you're decimating a 26-long sequence, if you select an even decimation, you will get back two 13-long sequences. Since we know we had a 26-long sequence to begin with, we want to wind up with a 26-long sequence, and even decimations won't do it for us.

Alright, that explains why we didn't try any even decimations. Why did we do just 3, 5, 7, 9, and 11? Why not 13?

With our 26-long sequence, if you decimate it by 13, you'd start at A, count down 13 to get a K, and then count 13 more to arrive back at A. If you decimate by 13, you'll end up with thirteen two-long sequences. Again, not a 26-long sequence, so we don't decimate by 13.

Why didn't I try some larger odd-length decimations? Well, if you decimated by 15, you'll get the same sequence as the 11 decimation, except in reverse. Same thing with decimation 17: it's the same sequence as the 9 decimation written backwards. Decimation 19 is just decimation 7 in reverse; decimation 21 is decimation 5 written in reverse; decimation 23 is the decimation 3 backwards; and decimation 25 is the original sequence written in reverse order. If we remember to consider the original sequence, as well as the decimation 3, 5, 7, 9 and 11 sequences in both forward and reversed order, we'll have all possibilities for the true sequence used.

That's fine, but which one of these possibilities is correct? Looking back at the previous section on how the sequence is constructed, it's extracted from a transposition matrix. The matrix with a keyword-mixed sequence based upon NEUTRAL and a hat of NONCOMMITTAL:

```
N  O  N  C  O  M  M  I  T  T  A  L
7  9  8  2 10  5  6  3 11 12  1  4
-------------------------------
N  E  U  T  R  A  L  B  C  D  F  G
H  I  J  K  M  O  P  Q  S  V  W  X
Y  Z
```

produced this sequence:

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

Notice that the letters V, W, X, Y and Z all land at the bottoms of columns. These are letters that are fairly infrequently used, and are thus not as apt to be found in the keyword, NEUTRAL in this instance, whose letters appear on the top line of the matrix.

If we look at where V, W, X, Y and Z appear in the 26-long sequence produced in this example:

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

You can see that these letters are pretty well spread out across the string of 26-letters, and are not all clustered together. This will be true of the original sequence used.

Additionally, pick two letters which should appear next to each other at the bottoms of columns of the matrix, for instance W and X. Look immediately to the right or left of the W and X. Do you find two other letters which might land next to each other alphabetically? Yes! Immediately to the left of W is F, and immediately to the left of X is G. F and G fit together nicely in a matrix of this form.

We looked to the left of W and X to find the F and G. If we had to look to the right of W and X to find two letters that would have fit nicely together, that would tell us that our sequence should be the reverse of what we were looking at.

If the end-of-the-alphabet letters are spread out across the sequence, and you can find letters immediately to the left or right of two letters you might expect to come together at the end of the alphabet (V, W, X, Y, and Z), then you have a good candidate for the actual 26-letter sequence used.

Let's return now to our 26-long sequence and its decimations to see if we can find one that has the properties for which we're looking. We'll place the V, W, X, Y and Z in **bold** for ease in locating the correct sequence:

	A D J T **Y** C G L P U **W** S O K **X** I B F E **Z** **V** N H M R Q
3	A T G U O I E N R D **Y** L **W** K B **Z** H Q J C P S **X** F **V** M
5	A C **W** I **V** Q **Y** U **X** **Z** R T P K E M J L O F H D G S B N
7	A L **X** N J U B M **Y** S E Q G K **V** D P I H T **W** F R C O **Z**
9	A U E D **W** **Z** J S **V** T O N **Y** K H C **X** M G I R L B Q P F
11	A S H L E T **X** Q **W** N G F J K R U **V** C B D O M P **Z** **Y** I

Of all these possibilities, which one looks best? Decimation 7 doesn't look too bad -- the V, W, X, Y and Z are pretty spread out. How about the letters immediately to the left or right of, say, Y and Z? Immediately to the left of Y is M, and the letter immediately left of Z is O. M and O go together well if N is used in the keyword. How about the letter immediately to the left of X? It's L. If X and Y go together, then L and M will go together. I think we've found the correct sequence. Let's see if we can't put it back into the matrix form used to create the sequence.

Here's our Decimation 7 sequence again:

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

Let's start by placing A L X as a column, and we'll place B M Y right next to it. That'll give us:

A B
L M
X Y

Underlining the sections we've used, we have this:

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

C O **Z** looks like a good guess for the column after B M **Y**, so let's place it there:

A B C
L M O
X Y Z

If we try placing H T **W** before the A L **X** column, we'll have a T coming right before an L, and that doesn't look good. Maybe W is used in the keyword somehow. If so, then we'd have V coming before X in the bottom of the matrix. G K **V** looks pretty good as it will place a K before the L on the second row:

G A B C
K L M O
V X Y Z

And again, underlining the sections we've used thus far:

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

N J U looks like it will fit nicely before the G K V column.

N G A B C
J K L M O
U **V X Y Z**

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

What comes next? If we put T before the U, we'll have H coming before J. That makes sense if I is in the keyword. Let's try it:

```
I N G A B C
H J K L M O
T U V X Y Z
```

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

We've already placed the G in the top row of the matrix as part of the keyword, so that won't land to the left of H. Going one letter back from G we get F. Let's place W F R next to I H T:

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

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

This looks good if S is used in the keyword as R and T come together on the third line. We still need to use S in the keyword, and the S E Q segment is still unused. Let's place it to the left of the W F R and see how it looks.

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

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

The only segment from our 26-long string that's unused is D P. It looks like it will fit nicely to the right of the C O Z column, so let's put it there:

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

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

And we did it! We have the matrix recovered, as well as the key that was used: SWING

Okay, we have a setting of SLIDE, and a key of SWING. The hat is still left to be recovered.

Next we need to determine the numeric key used to extract the columns from the matrix to form the 26-long sequence. The A L **X** stretch was the first segment pulled from the matrix, so place a "1" above that column in the matrix:

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

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

The N J **U** segment appears second in our sequence, so that column in the matrix gets a "2" placed above it:

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

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

Continuing in this fashion, B M **Y** came out next, so it gets a "3" above it in the matrix, S E Q gets a "4" above it, and so on:

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

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

We have a nine-long numeric key: 4 8 7 2 5 1 3 9 6. Now comes the really hard part. We need to find a 9-letter word or phrase with this numerical pattern, and has something pertaining to SWING and SLIDE.

There are two different paths one might consider here. SWING and SLIDE are both things that one might find on a playground, so maybe the 9-long hat is another piece of playground equipment. SWING and SLIDE are also baseball terms, so it might also be something pertaining to America's pastime.

Knowing of the Headline Puzzle Editor's affection for baseball (know thy target), you might try that direction first. Some nine-letter baseball terms are: CURVE BALL, GRAND SLAM, LINE DRIVE, SWITCH HIT, TWO BAGGER, and UPPER DECK. Checking these to see what numerical patterns they have, none have the 4 8 7 2 5 1 3 9 6 pattern for which we're looking.

Brainstorming to try to come up with other pieces of playground equipment, you might think of MONKEYBARS, LADDER, RINGS, CRAWL TUBE, SPRING RIDE, TETHER BALL, SEESAW, TEETER-TOTTER, BALANCE BEAM, MERRY-GO-ROUND, BALL PIT, and SAND BOX. Most of these are not nine-long. CRAWL TUBE doesn't have the 4 8 7 2 5 1 3 9 6 pattern, and neither does MONKEYBAR. Good effort though.

Eventually you might think of JUNGLE GYM, which does have the 4 8 7 2 5 1 3 9 6 pattern. We did it! We've solved all five headlines, and recovered the setting (SLIDE), the key (SWING), and the hat (JUNGLEGYM).

If you're still stuck on obtaining the hat, please see the next section for another technique that may prove useful.

Nice going! If you follow the work done in this example, you should have few problems, if any, in solving other Headline Puzzles. But just in case you do, the next section contains helpful hints and special things to be aware of.

4. Potential Problems and Helpful Hints

"I've solved two headlines and I'm having problems chaining to obtain a 26-long sequence. What do I do?"

In the example solution we worked through the July 2005 Headline Puzzle and with just two sets of chains we were able to piece together most of a 26-long Equivalent Primary Component. But, sometimes, you won't be able to use a good number of your chains. Let's look briefly at the July 2006 Headline Puzzle, and we'll see this phenomenon occurring. Let's assume you have the first two headlines solved:

```
    YANKS´ JOHNSON, TORRE EJECTED IN A TESTY AFFAIR
1.  EPQRJ´ KNYQJNQ, ONVVG GKGFOGH WQ P OGJOE PXXPWV

    ´UNCLE TOM´S CABIN´ WILL OPEN TO VISITORS
2.  ´CPDQI MAJ´V DKFXP´ ZXQQ ARIP MA NXVXMAOV


3.  NMXBT ZTJC KTFZBR, GFIGBT ZMRQR RPWBBYB XJQBTSBA


4.  MIJDP XRQ KRUU EPQJLPD KJDM'D EPCJPDB IW REXC


5.  Z. HBYAF'Z ZUYAZZ-NYKEAI FNNKVUKBI UB BIGKIA PFCKIP KZ ZXKHKIP
```

Placing the cipher values inside a matrix as we did before with the plain values across the top:

```
 P:  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

C1:  P   F H G X   Y W K R     Q N     V J O         E
C2:  K F D   I       X     Q J P A R   O V M C N Z
C3:
C4:
C5:
```

Chaining the plain line to the first and second lines of cipher in the matrix:

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

But what happens when we try to link these two sets of chains together to make a 26-long sequence? Let's arbitrarily make the second set of chains run horizontally, and the first set vertically:

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

Starting with SVNPROAK horizontally:

```
S V N P R O A K
```

(Again, chains we've used are now **bold**):

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

We can add AP, SJKRV and TONQ from the first set vertically:

```
    S
    J
    K           S
    R   A   T   J
S V N P R O A K
J         N P R
K         Q   V
```

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

Returning to the second set, we can add LQ and TMJ horizontally:

```
      S
  T M J
      K           S
      R   A   T M J
    S V N P R O A K
T M J         N P R
    K       L Q   V
```

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

And we're stuck at this point, unable to add any of the other unused chains from either of the two sets.

But looking at what we've done so far, there is some overlap (reused letters) on the lines. Let's try to combine them to see what we can get:

```
      S
  T M J
      K           S
      R   A   T M J
    S V N P R O A K
T M J         N P R
    K       L Q   V
```

If we start with this line:

```
                    S V N P R O A K
```

We have some overlap with the `T M J  N P R` line:

```
                    S V N P R O A K
      T M J           N P R
```

Combining, we get:

```
      T M J     S V N P R O A K
```

The `K  L Q  V` line overlaps:

```
      T M J     S V N P R O A K
    K       L Q   V
```

and combining gives:

```
    K T M J L Q S V N P R O A K
```

What's happened here? `K` has repeated, thirteen letters down from where it first appears. We have a 13-long sequence. If we take the unused chains from our headlines, we should be able to come up with another, different 13-long sequence. However, we must use the relationships the same way: the second set of chains must be written horizontally, and the first set vertically.

Once we obtain a second 13-long sequence we'll be able to combine them to make a 26-long sequence. But first, back to our original chains to construct the second 13-long sequence.

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

Let's start with EIX and we'll write it horizontally.

```
E I X
```

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

Adding CFX, DHYEG and IW vertically:

```
D
H   C
Y   F
E I X
G W
```

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

We can now add the remaining unused chains from the second set horizontally:

```
D
H U C D
Y B F
E I X
G W Z
```

```
1:  AP  CFX  DHYEG  IW  SJKRV  TONQ
2:  SVNPROAK  BF  UCD  EIX  LQ  TMJ  WZ
```

Here you might notice that in the first column we have DHYEG reading down. If we extend that to the D at the end of the H U C D line, and write DHYEG going down there, we get:

```
D
H U C D
Y B F H
E I X Y
G W Z E
      G
```

Now we can start combining rows which contain "overlapping" letters:

```
D
H U C D
Y B F H
E I X Y
G W Z E
    G
```

If we begin with:

```
G W Z E
```

and work our way up the grid, line-by-line, you can see lots of overlapping letters.

```
G W Z E
    E I X Y
        Y B F H
            H U C D
```

Combining all these together, we have another 13-long sequence:

```
G W Z E I X Y B F H U C D
```

Alright, we have these 13-long sequences, involving all 26 letters of the alphabet:

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

First of all, why did we get two 13-long sequences? The reason this happened is because the two headlines which were solved first just so happened to both be enciphered with the original sequence offset at an even distance. And until we actually solve a headline which has an odd-length offset, we won't be able to actually obtain a 26-long sequence.

So let's try to solve another headline and see if we can't somehow combine these two 13-long sequences into a 26. And despite having two 13-long stretches, we can still use them to help decrypt headlines.

Let's go back to the headlines from July 2006 and try to solve another headline.

```
    YANKS´ JOHNSON, TORRE EJECTED IN A TESTY AFFAIR
1.  EPQRJ´ KNYQJNQ, ONVVG GKGFOGH WQ P OGJOE PXXPWV

    ´UNCLE TOM´S CABIN´ WILL OPEN TO VISITORS
2.  ´CPDQI MAJ´V DKFXP´ ZXQQ ARIP MA NXVXMAOV


3.  NMXBT ZTJC KTFZBR, GFIGBT ZMRQR RPWBBYB XJQBTSBA


4.  MIJDP XRQ KRUU EPQJLPD KJDM'D EPCJPDB IW REXC


5.  Z. HBYAF'Z ZUYAZZ-NYKEAI FNNKVUKBI UB BIGKIA PFCKIP KZ ZXKHKIP
```

How about the fifth headline? I'd like that Z to be an S: the Z comes after an apostrophe, so S is a good candidate as part of a possessive pronoun, and the Z. at the start would make a good abbreviation for "South."

Looking at our two 13-long chains, Z and S happen to land in different sequences! This is good. Align the sequence with the Z beneath the one with S, matching up the S and Z:

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

If our guess is correct and Z decrypts to S, then everything in the bottom sequence should decrypt to the letter corresponding to it in the top sequence. Let's decrypt as much of the fifth headline as we can and see if it looks good.

```
    S. KOR A'S STR SS- R V N A    T ON TO ONL N   AM N   S SP K N
5.  Z. HBYAF'Z ZUYAZZ-NYKEAI FNNKVUKBI UB BIGKIA PFCKIP KZ ZXKHKIP
```

Looks great! That's almost certainly KOREA appearing before the apostrophe. If we take the K T M J L Q S V N P R O A sequence and align it with the other so the A is beneath the E, we should be able to decrypt the entire the entire headline. But keep the original alignment above, just re-write the K T M J L Q S V N P R O A sequence beneath what we already have, again aligning A with E:

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

Now, using the bottom line, we can read up to the second line to decrypt everything else in the fifth headline:

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

   S. KOREA'S STRESS-DRIVEN ADDICTION TO ONLINE GAMING IS SPIKING
5. Z. HBYAF'Z ZUYAZZ-NYKEAI FNNKVUKBI UB BIGKIA PFCKIP KZ ZXKHKIP
```

Alright, we have the fifth headline done. Now, how can we make a 26-long sequence? Using the three lines we have above, we have KHQ reading down the first column. There should be another column that has a Q at the top of it. Yep, five columns to the right is the QWR column. We can link the KHQ and QWR together to make:

```
K H Q W R..
```

Continuing in this fashion, there should be a column with R at the top of it, and sure enough, five columns to the right of QWR is RYM. Add it to what we have:

```
K H Q W R Y M..
```

To this we can add MCV (five columns to the right of RYM, notice a pattern happening here?), then VEA, etc. Eventually we get this 26-long sequence:

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

And we're back to K after the I. This 26-long sequence is an EPC of the original sequence used to encipher the headlines, and can be used in the same manner as we did when we solved the July 2005 puzzle. You may need to take decimations of it to recover the true 26-long sequence used, but you can use this 26-long sequence to help you solve the remaining headlines and recover the setting.

I don't want to spoil all your fun. I'll let you continue the July 2006 puzzle from here. I just wanted to show you what happens when you solve two headlines which are offsets of the original by an even distance. Until you encounter a headline enciphered at an alignment that's enciphered at an odd-length distance, you'll be left to play with two 13-long sequences.

"What if <u>all</u> the headlines are enciphered using even-distance offsets of the 26-long sequence against each other? How do I recover the original sequence when that happens?"

This will happen from time to time (approximately once every 39.2458 puzzles), and the task then is quite daunting as you'll have to make decimations of the 13-long sequences and then try to "weave" one of the 13-long sequences into the other at all 13 possible alignments, looking for a 26-long stretch that looks like it could come from a matrix. It's a very long process checking all the possibilities, but it is doable. So, let's show you how you'd go about doing it when the planets align and unthinkable occurs

For demonstration purposes, here's the February 1985 Headline Puzzle with all five headlines solved:

```
   ETHIOPIA HOPES FOR MILLIONS MORE IN NEEDED AID
1. QSZWVCWH ZVCQM YVB XWJJWVIM XVBQ WI IQQAQA HWA

   MANUFACTURERS ASSAIL PLAN FOR TAX REFORM
2. YSJQUSLZQVAVF SFFSRW KWSJ UPV ZSE VAUPVY

   JOHN DREW SUSPENDED BY UTAH JAZZ
3. KIDP XLFN QMQRFPXFX JZ MEUD KUAA

   FDA PLANS CAMPAIGN AGAINST FRAUDULENT MEDICAL DEVICES
4. AMX JVXBE RXQJXPWB XWXPBEY AKXSMSVZBY QZMPRXV MZIPRZE

   SCIENTIFIC PANEL SUPPORTS 'NUCLEAR WINTER' THEORY
5. FLRAJZRURL KSJAW FQKKPVZF 'JQLWASV BRJZAV' ZMAPVD
```

The resulting recovery matrix, with the plain arranged in A-Z order 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

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

In this puzzle, no matter which set of cipher and plain alphabets you select to chain, you'll always get two 13-long chains. It appears that the setting is the word KNOWN, appearing beneath the plaintext letter G. Knowing G is the first letter of the original sequence (it sits atop the setting), let's chain the Plain line to the first headline's cipher. In doing so, we get these two chains:

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

To blend these together, grab a letter from the first 13-long chain (how about "G" since we know it's the first letter of the original sequence). Then grab a letter from the second set (I'll pick "A" since it's first alphabetically in that 13-long set). Then, selecting the next letter in the first chain we get "K", then pick the next letter in the second chain "H" and so on, alternating back and forth.

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

Doing that, you get this 26-long sequence:

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

Next, we check to see if we can make a nice matrix from it. After highlighting the letters at the end of the alphabet (I've put them in bold), and using the same reasoning as before, we see this sequence is not going to work.

So, we need to repeat the process, but this time grab the "G" from the first sequence, and then grab second letter in the second sequence, "H", and again alternate back and forth between the sequences. Doing so, we obtain this sequence:

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

This still doesn't look good. Trying all other possible weavings with these two sequences, we get these possibilities:

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

Sadly, none of these look good either.

So, next we have to decimate each of the two 13-long sequences.

Decimating the first sequence by 3 we get: [G J P I V L B N O K R C W]. Decimating the second yields: [A F Q M D Z E S U H Y T X].

Do the same interleaving technique with these two decimated sets:

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

Grab G, then A, then J, then F, etc, and you get:

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

No good again. So we interleave the two 13-long chains again, but this time initially selecting the "F" from the second sequence. This gives us:

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

This still doesn't look like it came out of a matrix.

The process continues until we eventually come across the correct decimation and interleaving. This could be quick (if we're lucky), or could take a long time (if we're not so lucky). If decimation 3 of the sequences doesn't work, we try all the interleaving of decimation 5, and then 7, and then 9, and then 11.

If we continued from here, we're actually not far away from a solution. Here are the other possible interleavings with our original 13-long sequences on decimation 3:

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

Examining these possibilities, the sequence three from the bottom looks promising:

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

Immediately to the right of W is H. To the right of X is I. Next to Y on the right is J. And on the right of Z is K. With WXYZ all likely occurring at the bottoms of rows, and HIJK alphabetically above them, we've come across the right sequence.

Or have we? Since the HIJK letters near WXYZ are occurring on the right, we've actually come across the reverse of the correct sequence. So we need to re-write the sequence in reverse order, but still beginning with G, the first letter of the original sequence.

Doing so, we obtain this sequence:

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

Reassembling this into a transposition matrix we get:

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

When all headlines are at even-length offsets, it can be a laborious task to decimate and weave the two 13-long chains together, checking all possible resultant 26-long sequences.

If this event happens, and it's bound to come up sooner or later, you'd almost certainly want a computer program to do all the work, displaying all the possible interleavings and decimations.

If you're a programmer, I encourage you to write a program to accomplish this task. But, if you're working on a linux or Unix computer and can run Python programs, I have such a program that I wrote when I took a Python class. If you'd like a copy of my program, which is nothing fancy but gets the job done, send me an e-mail, and I'll happily send it along to you.

Good luck! That is indeed nasty when it's all even-length offsets.

"I'm still having trouble getting the hat. Do you have any help for that?"

Yes, and I have to tip my "hat" (no pun intended) to some kind folks from Australia for showing me this method for trying to figure out hats. Because of their generosity, I'll call this the "Australian method" or "Aussie method."

Let's look back at the February 1989 Headline Puzzle. While recently re-solving this puzzle, and drawing a blank on the hat, I used the same technique suggested by our colleagues "down under."

The setting for the February 1989 puzzle was `SMITH`, and the key was `GLADYS`. The hat was 12 characters long, and had this order: 7 1 10 12 9 5 2 6 4 8 11 3.

I was stumped and a search using Google and Wikipedia didn't turn up any immediate possibilities for a woman named Gladys Smith. So I used the Aussie method for obtaining the hat.

The Australian method for finding the hat is as follows:

Step 1. Enumerate the alphabet in 0-25 order, with A=0, B=1, etc., up to Z=25.

Step 2. Take the key obtained from the hat, and subtract one from each of the values.

Step 3. If the hat is nine letters or shorter in length, triple each of the values obtained in step 2. But if the hat is ten letters or longer, double the values.

Step 4. Using the numerical representation of letters established in Step 1, replace the numerical values calculated in Step 3 with the letter which corresponds to each of the numbers.

Step 5. Assuming the letters used in the hat are fairly evenly distributed, the results from Step 4 should get you in the "neighborhood" of the actual letters used in the hat. Writing out the four letters that precede and follow the letters you got in Step 4, and scanning a bit should lead you to the solution.

Let's try it with my recently re-solved puzzle from February 1989.

Step 1.

First, enumerate the alphabet in 0 - 25 order, with A=0 and Z=25:

```
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
0  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
```

Step 2.

Next, take the key obtained from the hat, and subtract one from each of the numbers. For the February 1989 puzzle, the numerical key for the hat was 7 1 10 12 9 5 2 6 4 8 11 3, so subtracting one from each digit, we get:

```
6 0 9 11 8 4 1 5 3 7 10 2
```

Step 3.

Since the hat is 12 letters long, we double the values obtained in Step 2:

```
12 0 18 22 16 8 2 10 6 14 20 4
```

Step 4.

Next we replace the numbers obtained in Step 3 with their letter equivalents from Step 1.

12	0	18	22	16	8	2	10	6	14	20	4
M	A	S	W	Q	I	C	K	G	O	U	E

This establishes **M A S W Q I C K G O U E** as the "base" for attempting to find the hat.

Step 5.

Writing the four letters that come before and after each of our "base" values, we get this:

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

Scanning up and down from the "base," and trying to form letter combinations that would occur in English, eventually you can see this emerging from the murky mist:

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

MARY PICKFORD is the hat.

As you can see, this method worked pretty well in this instance. The farthest away from the "base" that any of our letters was from the true letter value was three (the R was three letters away from the U in the base). And the base letters were exactly right in six of the 12 positions!

However, you never know when the diabolical Headline Puzzle editor will do something nasty, like I did in September 2010. That month the setting was MESSY and the key was JUMBLED. The hat had a numerical key of 5 1 2 4 9 6 7 3 8 10. It turned out the hat was TOPSYTURVY, which contains only letters from the second half of the alphabet. This makes the Aussie method a bit problematic in this case, but this is the exception rather than the rule. This technique is a neat trick that works most of the time to get you in the "vicinity" of the letters used in the hat, and I heartily recommend it if you're stuck.

"I've solved all the headlines, and after double-checking everything, I still can't find the setting. What should I do?"

Well, every once in a while, this will happen, and most likely you haven't done anything wrong. It's just that the editor made a modification to prevent one or more headlines from enciphering to itself.

For instance, what would happen if the words used for the setting, key and hat were WHIST, PINOCHLE and CRIBBAGE respectively, all of which card games. (These were the setting/key/hat words used in April 1994). Watch what happens when you create the 26-long key, and align the headline cipher alphabets.

Starting with the hat of CRIBBAGE, we create the transposition matrix by writing a keyword-mixed sequence based on PINOCHLE into the eight-columns-wide matrix:

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

Extracting the columns according to the hat's numeric key, we obtain a 26-long sequence of:

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

Now, writing the setting beneath the first letter in the sequence and aligning the 26-long sequence, this matrix is produced:

```
 P:   H J V O F T C G U P A Q Y E M X L K W N D S I B R Z
-----------------------------------------------------------
C1:   W N D S I B R Z H J V O F T C G U P A Q Y E M X L K
C2:   H J V O F T C G U P A Q Y E M X L K W N D S I B R Z
C3:   I B R Z H J V O F T C G U P A Q Y E M X L K W N D S
C4:   S I B R Z H J V O F T C G U P A Q Y E M X L K W N D
C5:   T C G U P A Q Y E M X L K W N D S I B R Z H J V O F
```

What happens when the second headline is enciphered? Every character in the plain text of headline #2 will encipher to itself. Rather than having gibberish to decrypt, the headline's plain text would appear in its entirety!

Many puzzle solvers would consider this a serendipitous bonus as there is one fewer headline to decipher! But, alas, the Headline Puzzle editor doesn't want to deprive anyone of the fun of recovering all five headlines. Thus, a technique, first developed by Paul Derthick and then continued by Larry Gray and myself, was implemented that usually gets around the problem of plain and cipher crashes, and still allows the editor to still use the three words intended for the setting, key and hat.

The technique involves three inversions:

1) The transposition matrix from which the ordering of the 26-long sequence is still used, and with the same numerical key for the hat. But instead of extracting the columns from top-to-bottom, they're pulled out from bottom-to-top. This makes the 26-long sequence which is then used in the encipherment matrix, and is the first "inversion" implemented.

2) Next, the matrix is inverted so the cipher is placed on top and the plaintext for the five headlines is contained within. That's the second inversion.

3) Finally, the setting is inverted so it appears as it if were written backwards (or reading upwards) beneath the first letter of the 26-long sequence.

Usually, by using these three inversions, the same setting, key and hat can be used and will eliminate the crashing.

Let's go back and follow the same steps that Larry did in July 1994.

1) Extract the columns in the transposition matrix from bottom-to-top.

Here's our matrix again:

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

Instead of pulling out `H J V` underneath the "1", we pull out the letters from the bottom, producing `V J H`. Then, under the column labeled with "2", we pull out `T F O`. Continuing in this fashion, we obtain this as our 26-long sequence:

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

2) Construct the matrix with the cipher on top and plain within.

That's easy enough:

```
 C:   V J H T F O U G C Y Q A P X M E W K L S D N Z R B I
-----------------------------------------------------------
P1:
P2:
P3:
P4:
P5:
```

3) Write the setting into the matrix in reverse order beneath the first letter in the 26-long sequence, and align the alphabets accordingly.

```
 C:   V J H T F O U G C Y Q A P X M E W K L S D N Z R B I
-----------------------------------------------------------
P1:   T F O U G C Y Q A P X M E W K L S D N Z R B I V J H
P2:   S D N Z R B I V J H T F O U G C Y Q A P X M E W K L
P3:   I V J H T F O U G C Y Q A P X M E W K L S D N Z R B
P4:   H T F O U G C Y Q A P X M E W K L S D N Z R B I V J
P5:   W K L S D N Z R B I V J H T F O U G C Y Q A P X M E
```

And voilà! The crashing has disappeared.

The same techniques for solving the headlines that you learned in the main section of this tutorial still apply. Chaining will work the same, as will recovery of the 26-long sequence. But if you don't see a five-letter word reading downward in the enciphering matrix when you have plain text on the top, try rewriting the matrix so the plain is inside the matrix and the cipher sits on top. Then scan upward to see if any of the columns contain a five-letter word. If so, whatever cipher letter the setting sits beneath is the initial letter of the 26-long sequence.

It may get a bit tricky when reassembling the transposition matrix, but just keep in mind that the columns were extracted from bottom-to-top, and so the correct decimation of the sequence will fit nicely into the matrix in bottom-to-top order.

This technique is a nice twist which allows the headline puzzle creator to avoid having to discard a great setting/key/hat combination just because it caused a crash. Usually (but not always), these three inversions will prevent the crashing from happening. However, if there are still crashes, even with the inversions implemented, some other devilish technique may need to be introduced without warning. Stay on your toes, puzzle solvers!

5. Questions for the Headline Puzzle Editor

From what newspapers do you select the headlines?

Living in Pennsylvania and commuting an hour to work each day (yes, I'm one of those), I get and read The Philadelphia Inquirer and The York Daily Record each day of the week. So I select most of the headlines from those two papers. The local headline usually comes from the York paper as they tend to have more Maryland, Baltimore and DC news than the Philadelphia paper. But if I'm in a pinch, I might go on the Internet and select a local headline from the on-line version of The Baltimore Sun or The Washington Post. Most of the time I can find what I need between the Philadelphia and York papers though.

My selection of newspapers can cause a "non-regional" flavor though. For example, a September 2004 headline I used read: `D.C. SUBWAY RIDER ARRESTED FOR EATING CANDY BAR`. You can tell this wasn't selected from The Washington Post as it would almost certainly be called the "Metro" rather than the "D.C. Subway" in a more local paper.

How timely are the headlines which are selected?

Back in the old days when the Headline Puzzle appeared in the NSA Newsletter, Paul Derthick and Larry Gray had to select them about six to eight weeks in advance of the publication date. But with the Headline Puzzle's own Wiki page, new Headline Puzzles now appear on the first working day of each month. This means I can select headlines right up to the day I create the puzzle, making them much more timely than Paul or Larry ever could.

If a headline catches my eye early in the month that has potential for making the puzzle, I'll hold on to it for consideration. Otherwise, I'll usually wait until mid-month before I really start looking in earnest for headlines to use. I never hold on to a potential headline after I've made the puzzle. This means my headlines are relatively fresh, usually within two to three weeks of the puzzle's publication, and sometimes even within a week.

How do you pick your headlines?

I need to select one headline from each of the five categories: International, National, Local, Sports, and Business. Other than that, I like choosing headlines that have alliterations (lots of words starting with the same letter) or rhymes, or some funky spellings of proper names. These tend to make breaking into the headlines by frequency counts harder -- the most common letter might not necessarily be an E or a T or an N.

Also, those crazy foreign place names (KYRGYZSTAN, OUTAOUAIS, etc.), tend not to be found in people's word pattern lists, so trying to break into the headlines through them is often fruitless. Seeing a place name like this immediately sets off bells and whistles with me, and you can bet I'll include it in the next headline puzzle, unless I have something better in that category. We don't want the puzzle to be too easy, right?

Additionally, I want to select headlines that hopefully don't offend anyone. I'll intentionally try to stay away from a headline dealing with a political issue or candidate, or headlines which are just gruesome. It's a big downer if you work hard to solve a headline only to find out that seven people died in a fiery crash. That won't happen with my puzzles, I promise.

When I first began as Headline Puzzle editor, I wanted headlines that would challenge the solver, regardless of the obscurity of the event described in the headline. But as I began to work through the past puzzles created by Paul Derthick, I encountered headlines about man landing on the moon in 1969, the Watergate scandal in 1973 and 1974, and the U.S. winning gold in hockey at the 1980 Winter Olympics. These were all events that I remembered happening as I grew up, and I realized that the headlines used were providing a nice timeline of history.

As a result, I now try to select headlines that punctuate top news stories for the month, so 30 years from now, someone returning to solve my old puzzles might have the same recollections of past events as I did.

Do you ever not use headlines from newspapers?

Yes. There's a neat tradition started by Larry Gray that every April puzzle consists of phony headlines, our April Fools joke to the puzzle solver. Here's an example showing the headlines from the April 2004 puzzle:

1. BLUE CRABS SCARCE IN CHESAPEAKE, MILLIONS OF MARYLANDERS FACE STARVATION
2. SCHICK INTRODUCES 'THE SEPTER,' NEW RAZOR WITH SEVEN BLADES
3. REDUCING BUDGET COSTS, TWO STATES MERGE TO FORM 'ARKANSIPPI'
4. UMBC ADVANCES TO FINAL FOUR IN NCAA CROQUET TOURNEY
5. COLOMBIA, BRAZIL FORM ORGANIZATION FOR COFFEE EXPORTING NATIONS: OPERK

But note that some traditions never die as there is a fake headline from each of the five categories: International, National, Local, Sports and Business.

Occasionally, in the past, old headlines have been used to commemorate an event. For instance, in June 1976, the headlines were selected throughout U.S. History in honor of the Bicentennial. These headlines were "fabricated" by Paul Derthick and not extracted from any newspapers, but did accurately reflect important historical events.

6. A Final Word From the Editor

Hopefully this tutorial has been helpful to both the newcomer to the Headline Puzzle, as well as master solvers who have many years of experience. If anyone has questions or comments about this tutorial, the current puzzle or any past puzzles, or is just plain stuck, please, I welcome you to contact me.

It's nice to see new people each month attempting to solve the puzzle for the first time, and I delight in hearing from tyros who've just solved the puzzle in its entirety.

I'm thrilled to be the steward carrying forward this NSA tradition, and hope that I can live up to the high standards originally established by Paul Derthick and continued by Larry Gray. It is my hope that this monthly puzzle will continue forward in perpetuity, long after my days at NSA have concluded.

Good luck! Have fun!

APPENDIX

Below is a list of common two- and three-letter words in English, which may be helpful to those solving the Headline Puzzle:

Common two-letter words

AM	BE	HE	IT	OF	TO
AN	BY	IF	ME	ON	UP
AS	DO	IN	MY	OR	US
AT	GO	IS	NO	SO	WE

Common three-letter words

ACE	BID	FIT	JOB	OUR	THE
ACT	BIG	FIX	KEY	OUT	TRY
AGE	BIT	FLY	LAW	OWE	TWO
AGO	BOX	FOR	LAY	OWN	USE
AID	BOY	FOX	LED	PAY	VAN
AIM	BUT	GAS	LEG	PER	WAR
AIR	BUY	GET	LOT	PRO	WAS
AND	CAN	GOD	LOW	PUT	WAY
ANY	CAR	GOT	MAD	RAN	WHO
APT	CUT	GUN	MAN	RED	WHY
ARE	DAY	GUY	MAY	ROB	WIN
ARM	DID	HAD	MEN	RUN	WON
ART	DIE	HAS	MET	SAW	YES
ASK	DRY	HER	NET	SAY	YET
BAD	DUE	HIM	NEW	SEA	YOU
BAG	EAT	HIS	NOT	SET	
BAN	END	HOT	NOW	SHE	
BAR	FAN	HOW	OFF	SIX	
BAY	FAR	ITS	OLD	TAX	
BED	FEW	JET	ONE	TEN	