AZBY-SHIFTWORDS: EDIFY, STORY

RICHARD SABEY
Chelmsford, England
richard_8978_sabey@hotmail.com

The atbash cipher (or athbash, under which name Web3 defines it) is a Hebrew substitution cipher which replaces the first letter of the Hebrew alphabet (aleph, א) by the last (tav, ת), the second (beth, ב) by the last but one (shin, ש), and so on, until we get to the last (tav, ת), which is replaced by the first (aleph, א). Jan Anderson described it in "Fledge Ledge Edge" (WW 8.1997-229). Naturally, the idea can be applied to our alphabet; following the precedent set by "atbash", I name it the azby cipher.

In the azby cipher, GIRL becomes TRIO and BRIGS becomes YIRTH. Rex Gooch termed words related in this way "word pairs with corresponding letters complementary" in his article "Complementary Letters and Words" (WW2.2002-70).

The azby cipher can be combined with the *n*-shift. Here, for example, is the azby-9-shift:

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

If *n* is even, all letters change. If *n* is odd, then letters (*n*+1)/2 and (*n*+1)/2+13 are unchanged. Each azby-shift is self-inverse, i.e. if you apply it twice in succession, the result is what you started with.

The longest words that azby-shift to words are 8 letters long:

```
pewterer(9)temperer    Purupuru(9)torotoro    hospices(23)piehouse
```

Some words that anagram each other azby-shift to each other, e.g. DUENDE(6)ENDUED. Because any azby-shift process is self-inverse, so is the permutation in this case: it thus consists of pairing some of the letters in one word, and swapping the letters in each pair to obtain the other word. For example, in DUENDE and ENDUED, the N and U pair, and each D pairs with an E. If anagrams of odd length azby-*n*-shift to each other, e.g. PALET(5)PETAL, then an odd number of letters remain unpaired and thus unchanged. This means that *n* is odd.

A word cannot *n*-shift to itself. It can azby-*n*-shift to itself, but only if *n* is odd and the word consists entirely of occurrences of the two letters that are left unchanged, e.g. BOOBOO(3).

As with shiftgrams, so here, chance brings together words which go well together. For example, that person who introduces himself to you sycophantically is a CREEPER(9)GREETER. That uncontrollable spasm you get from overusing the remote control is ZAPPER(9)JITTER. "Idiot's

Guides" and books for "Dummies" are DUFFER(9)FODDER. A cinematic biography is a FILM(17)LIFE. A cassette player's eject button makes the TAPE(24)EXIT. Equally, chance brings together words which one would never expect together: DIRGE(9)FARCE.

Azby-shift-reversals

The azby cipher can be combined with reversal. BOORISH and SHRILLY become each other. This process can transform a word into itself; the length of such a word must be even. In "Balanced Words" (WW11.1994-210), Susan Thorpe gave the examples POLK, KLOP-KLOP and WIZARD.

All three kinds of operation can be combined, to give an azby-shift-reversal. All azby-shift-reversals are self-inverse.

There is a pair of 9-letter words which azby-shift-reverse to each other, but no other example of words longer than 7 letters:

```
unshaping(1)unslating      asialia(1)Aspasia   Brendan(5)rebrand
                           abetted(5)ballade   Epirote(9)epirate
```

Only if n=13 can a word n-shift to its reversal. However, a word can azby-n-shift to its reversal for any n, though n must be odd if the word's length is odd. Although there is no pair of 8-letter words which azby-shift-reverse to each other, remarkably, there are 7 8-letter words which azby-shift-reverse to themselves. Two 7-letter words do, too.

```
unsewing(1)     chin-chin(16)    crotchet(22)        redefer(9)
maleates(5)     bathmats(20)                         secluse(23)
anesthyl(12)    Quaequae(21)
```

There is a pair of words that anagram each other, and that also azby-shift-reverse to each other: FEEDER(9)REFEED, showing that, if REFEEDER existed, it would azby-9-shift-reverse to itself. FLUSHY's azby-12-shift is GARTEN and its azby-25-shift-reverse is ARGENT; these last two words are remarkable in that they are mutual anagrams that 13-shift-reverse to each other.

Related words? WORK(3)SLOG. An attempt to cheat in a competition is a COMP(7)RUSE. Anyone foolish enough to try one, who fails, is a POOR(3)LOON. The contestant in the LEAD(5)BEAT the rest.

Azby-shiftgrams

Naturally, azby-shifting, like shifting, can be combined with anagramming. The set of azby-shiftgrams is even more impressive than the set of shiftgrams; there are typically nearly as many azby-shiftgrams as shiftgrams of one letter fewer. There is one 13-letter azby-shiftgram, EXTRAVAGATING(9)VICE-PRINCIPAL.

Among azby-n-shiftgrams, there is a greater contrast between the most and least prevalent n than there is among n-shiftgrams. For example, there is one azby-4-shift with 8-letter words, and none

with longer. Here is a type-collection of azby-*n*-shifts, including, for each *n*, one of the longest examples.

```
 9 hornbills      (0)moorishly          11 albumenizes (13)albuminizes
12 lymphangitic   (1)staphyloncus        9 handcraft   (14)unwalking
10 munitioned     (2)phytotoxin          9 blockages   (15)meadowink
11 bicorporeal    (3)uncolorably        11 overcheaply (16)unrepliably
 8 dram-shop      (4)moldwarp           10 coeminency  (17)discommode
12 lantern-jawed (5)veratralbine        10 adnexopexy  (18)untrounced
10 unscalably     (6)unshuffled         10 bargepoles  (19)rhabdosome
12 processioner   (7)spectroscopy       12 prelatically(20)triplicative
 9 staghound      (8)tubaphone          12 arithmograph(21)dumbfounding
13 extravagating (9)vice-principal      11 unretrieved (22)cranberries
 9 scrubbing     (10)whipbirds          12 lexicologist(23)soliloquized
 9 ridgewise     (11)Scotch egg          9 fitting up  (24)skippered
12 philarchaist (12)well adjusted       9 Huygenian    (25)squallery
```

BARGEPOLES may be replaced by its anagram PORBEAGLES.

Only if *n*=13 can a word *n*-shift to one of its transposals (unless a word is found which transposes to acegikmoqsuwy). However, a word can azby-*n*-shift to one of its transposals for any *n*, though *n* must be odd if the word's length is odd. Here are some of the longest words that azby-shiftgram into themselves:

```
13 prevaricating(9)    11 Westphalian(1)    10 papaphobia(16)
                          unpriceably(3)
12 undertakable(5)        stampedable(5)
```

Azby-shifts on the word calculator

In "The Word Calculator" (WW 5.1988-119), Dave Morice described a cylinder, held with its axis running from left to right, with strips, each with an alphabet on it, wound round it. If the alphabets are lined up so that all the A's are in a row, then a string of letters can be plotted by locating its first letter in the leftmost ring, its second letter in the next ring, and so on. Then shifting corresponds to rotating around the cylinder's axis. For example, a 13-shift is a 180-degree rotation about the axis. Applying an azby-shift corresponds to reflection about a plane that goes through the axis. Applying an azby-shift-reverse corresponds to a 180-degree rotation about a line that cuts the cylinder's axis at right-angles, flipping the cylinder end for end. Any reflection or 180-degree rotation is self-inverse. This illustrates geometrically why the 13-shift, all azby-shifts and all azby-shift-reversals are self-inverse.

Here's how to use Dave Morice's word calculator to apply azby-shift ciphers to a word. Use the rightmost strip as a reference strip. Set the first strip so that its A is level with the word's first letter in the rightmost strip. Repeat for the other letters. (Dave's illustration shows the cylinder being used to azby-shift the string LWYAN.) Now scan the strips for words. Suppose you found one level with the *n*th letter in the rightmost strip. That shows that it's azby-*n*-shift that transforms each of the words into the other. (I used a spreadsheet that display the alphabet, permuted as necessary, in columns. It works in a similar way to the word calculator. It's fine for

checking results of shifts and azby-shifts, and it's just as good as the word calculator at showing *accidental* finds. I can assure Dave and others who might try the word calculator that a computer program is a far more appropriate tool to use to do a systematic, comprehensive *scan* of a word stock.)

What next?

Shiftwords, shift-reversals, shiftgrams, azby-shiftwords, azby-shift-reversals, azby-shiftgrams... Has this seam been mined completely? Not at all. A shift cipher ciphers the alphabet as a string where each letter is followed by the letter 1 step forwards from it in the (cyclic) alphabet. With an azby-shift cipher, it's 1 step backwards. There are 10 more possible step sizes to try.

Readers will no doubt invent still more substitution ciphers to use instead of those which I have considered, thus further increasing the scope of transformations allowed from word to word. Close to the ultimate increase of scope is where the only restrictions on the cipher are that it not be polymorphic (i.e. that it encipher different letters as letters different from each other) and that it encipher each letter α as a letter different from α. In this case, the equivalent of shiftwords is non-crashing isomorphs (see WW73-146). Whether this restriction is applied, or whether the full range of non-polymorphic substitution ciphers is allowed, the equivalent of shiftgrams is words with the same letter distribution (see WW74-205).

I have remarked elsewhere that some shift-ciphers are more fruitful than others at producing shiftgrams. Generalising now to all non-polymorphic substitution ciphers: which are *least* fruitful, with respect to a specified word set? Is there one which doesn't enable any, say, 6-letter word to encipher into a transposal of a word?

All words are in Webster's 2nd or 3rd Unabridged, or UKACD16 (the 16th version of the United Kingdom Advanced Cryptics Dictionary).

Copyright © 2003 Richard Sabey