

Ciphers and Structures

Alex J. Quiz
Glendale, California

Ciphers are very interesting forms of wordplay. We will be going over 3 different kinds of ciphers. The first one is the Caesar cipher, or lettershift, discussed in November 1979 in "Alphabetic Letter-Shifts", in February 1990 in "Letter-Shift Words in the OSPD", and in the August 1993 Colloquy. The second one is the Atbash cipher, or balanced word pairs, discussed in February 2002 in "Complementary Letters and Words", November 2004 in "Balanced Word Pairs", and February 2005 in "More Balanced Word Pairs".

The third one is the Atbash plus Caesar cipher. It combines the Atbash and Caesar ciphers by applying the Atbash cipher and then the Caesar cipher on a word. An article in February 2004, "Azby-Shiftwords", has explored this form of wordplay but we are exploring it further. Also, there is another form of wordplay called the structure. It is very similar to difference words, but different also.

First, the structure. To take the structure of a word, we first change all of the letters into numbers, for example "people" becomes 16, 5, 15, 16, 12, 5 because those are the positions of the letters in that word in the alphabet. Then, we subtract each one from the one after it, adding 26 if needed.

So, 5 (or 31) - $16 = 15$, $15 - 5 = 10$, $16 - 15 = 1$, 12 (or 38) - $16 = 22$, and 5 (or 31) - $12 = 19$.

We can't subtract the letter after from the letter before like in difference words, we can only subtract the letter before from the letter after. Now, the differences are 15, 10, 1, 22, and 19. Now, we convert them back into letters. We change it into O, J, A, V, S. So, the structure of "people" is "ojavs".

Also note that the structure of "ing" is "es", making for some structure pairs because both are very common word endings.

There are 3 categories of structure words.

1. The words where their structure is all one letter.
2. The words that share their structure with another word.
3. The words where their structure is another word.

There are 25 categories of words where their structure is all one letter (not counting "z" because that would just be a word of all the same letter since Z is an increase of 0), for example "dins":

"dins" becomes 4, 9, 14, 19, and $9 - 4 = 5$, $14 - 9 = 5$, and $19 - 14 = 5$. Since the differences are 5, 5, 5, the structure of "dins" is "eee".

These words are listed with their structures next to them.

4 letter words -

filo (ccc), dins (eee), muck (hhh), clud (iii), zira (iii), tepa (kkk), coam (lll), anan (mmm), bobo (mmm), erer (mmm), lyly (mmm), nana (mmm), vivi (mmm), peti (ooo), ariz (qqq), dulc (qqq), jari (qqq), bung (sss), keys (ttt), and urol (www).

5 letter words -

mucks (hhhh), tepal (kkkk), anana (mmmm)

There are no longer words that have a structure of all one letter, even though there is an anime named

"Bobobo-bo Bo-bobo" with a structure of 13 Ms in a row, though that shouldn't count as a word. We also constructed a sentence like that, "Go, we muck SAI", which has a structure of 10 Hs in a row.

The words that share their structure with another word are just Caesar cipher pairs, for example "abjurer" and "nowhere" both have a structure of "ahkwmm". We'll talk about those later.

These are the words where their structure is another word. I'm guessing that most of them will be "ing" → "es" pairs.

6 letter to 5 letter pairs -

loping → cases, pungle → esses, alders → krama, reflux → mafic, declan → axiom, coping → lases, oracle → cibis, tumefy → arras, achmed → beery, eldest → grana, metion → roofy, hoping → gases, unwits → silky, elders → grama, erased → mirly, shades → oscan, estive → naomi, knives → cumin, refoot → maize, buzzes → sezen, boxing → mikes, coxing → likes, howlan → ghoom, afraid → elihu, acopic → blast, deinos → adead, ruced → chewy, fixing → cokes, noshes → adown, sluing → sines, moppet → bazoo, washes → drown (this one kind of makes sense), infand → erump, nablas → major, abdest → abana, sixing → pokes, widest → luana, sabirs → hagia, abdias → aberr, pewing → orles, elding → grees, fluing → fines, dewing → arles, jingle → yeses, lethia → sonar, moping → bases, slatch → sosie, fjords → declo, undeaf → spave, ingram → eskil, owling → howes, poppet → yazoo, poxing → yikes, kotyle → deems, wefted → hanky, rowlet (Who knew my dictionary contained Pokemon names?) → whoso, tapers → gooma

7 letter to 6 letter pairs -

anselme → melgar, falutin → ukiyoe, lenapes → simoon, ordered → clammy
Ordered → clammy is the longest common pair.

Weird facts about structure:

If you Caesar cipher a word, the structure stays the same.

If you Atbash cipher a word, the structure gets Atbash ciphered and then Caesar ciphered by a shift of 25, or Atbash plus Caesar with a shift of 25.

If you Atbash plus Caesar cipher a word, the structure gets Atbash plus Caesar ciphered with a shift of 25.

If you reverse a word, the structure gets Atbash plus Caesar ciphered with a shift of 25, then reversed.

If you arithmetic shift a word (talked about in February 2006 in "Shifts Progress"), the structure gets Caesar ciphered with the same shift as the arithmetic shift was. We won't talk about the arithmetic shift in this article however (or should I say Vquever, the VQ word for the digraph list?). We might talk about arithmetic cipher in the fall 2020 edition of Word Ways though.

Now, the Caesar cipher, or lettershift. It was discussed in November 1979 in "Alphabetic Letter-Shifts", in February 1990 in "Letter-Shift Words in the OSPD", and in the August 1993 Colloquy. It basically is just about shifting every letter by the same amount in the alphabet.

We won't go through all of the pairs in this one, just the 5-letter and longer pairs. If you want the 4-letter pairs, go to "Letter-Shift Words in the OSPD" in the February 1990 Word Wways. There are 3 sets of 4 5-letter words that shift into eachother:

cheer, diffs, jolly, and purre (even though no dictionary seems to have all 4 of them)

aneer, boffs, hully, and narre

dolls, groov, jurry, and wheel

There is also a set of 3 6-letter words that shift into each other, but one is an acronym, one is a place name, and one is an obsolete word: ARBTRN, Neogea, and riskie (obsolete form of "risky"). A 4-word set (Cleely, pyrryl, rattan, and vexxer) has not been used because one is a name and one is slang.

1-shift -

adder → beefs, aneer → boffs, cheer → diffs, shads → tibet, sheer → tiffs, sneer → toffs, steer → tuffs, anteed → bouffe, steeds → tuffet

2-shift -

bylaw → dancy, osmic → quoke

3-shift -

cobra → freud, dolls → groov (archaic 'groove'), groov (archaic 'groove') → jury (form of 'jury'), teloi → whorl, primero → sulphur (a famous pair)

4-shift -

alkyd → epoch, banjo → ferns, bejan → finer, danio → herms, ganja → kerne, lutea → pyxie, pecan → tiger, ratan (rattan?) → vexer, taney → xeric, three → xlvii (47), ganjah → kernel, lallan → pepper, Leanna → Pierre (both names)

5-shift -

admin → firns, fizzy → kneed

6-shift -

ahull → gnarr, boffs → hully, bolls → hurry, buffi → hallo, bulls → harry, butyl → hazer, chain → ingot, diffs → jolly, dolls → jury, fills → lorry, filly → lorre, fulls → larry, ginny → motte, golly → murre, gulfs → marly, gulls → marry, gummy → masse, gunny → matte, hully → narre, jimmy → posse, jinni → potto, jinns → potty, johns → punty, linum → rotas, luffs → rally, mills → sorry, mocha → suing, molas → surgy, muffs → sally, mulch → sarin, mumms → sassy, munch → satin, noggs → tummy, nulls → tarry, nutty → tazze, pulpy → varve, viola → bourg, vitim → bozos, wiles → corky, wolfs → curly, wombs → cushy, alohas → grungy, bombyx → hushed, fusion → layout, fusions → layouty (A word I invented for my unreleased book "Plop" about ciphers), wiliwili → corocoro (The longest pair known so far.)

7-shift -

aneer → hully, cheer → jolly, hotel → ovals, later → shaly, latex → shale, oxtter → vealy, tenet → alula, timer → aptly, wheel → dolls, inkier → purply, manful → thumbs, unfiber → bumpily

8-shift -

loads → twila, scans → akiva, setal → ambit, tsars → baiza

9-shift -

jerky → snath, river → arena, sleep → bunny, wiver → frena, xeric → gnarl

10-shift -

cubed → melon, dumbo → newly, Herod → Robyn, hesse → rocco, ruddi → benny, secco → commy, sewed → cogon, uredo → ebony, budded → lennon, muumuu → weewee

11-shift -

drips → octad, hints → styed, raphe → clasp, spits → dated, spots → dazed, trips → ectad, splits → dawted

12-shift -

didos → pupae, dirum → pudgy, dobro → panda, hoggs → tasse, sachs → emote, torus → fadge

13-shift or rot-13 -

cheer → purre, clerk → pyrex, craal → penny, creel → perry, dhoon → qubba, Ebola → Robyn, frere → serer, gnarl → taney, green → terra (this one actually makes sense), junes → wharf, becuna → orphan, cheery → purrel, Cheryl → purely, farrel → sneery, abjurer → nowhere (the most famous pair) In addition, gnat → tang is a reverse pair, and irk → vex are a synonym pair, along with cheer → jolly and green → terra.

There are no 14-25 shift pairs because those are just the reverses of the other pairs.

The 7-letter pairs are primero → sulphur, fusions → layouty, unfiber → bumpily, and abjurer → nowhere. The only 8-letter pair is wiliwili → corocoro.

Also, you can shift the sentence: "Navy be nowhere, one green"

And you get this sentence: "Anil or abjurer, bar terra"

Now we have the Atbash cipher. You have to subtract the position of each letter from 27, so A becomes Z, B becomes Y, E becomes V, G becomes T, and so on. The gnat-tang pair of this cipher is girt-trig.

We're not going to go over the pairs in this, because we're getting to the atbash plus caesar cipher. The Atbash plus Caesar cipher is that this article is mainly about. An article in February 2004, "Azby-Shiftwords", has explored this form of wordplay but we are exploring it further.

There are pairs from any shift from 1-25 because if you apply the same shift again, you get back to the original word. That means that words can Atbash plus Caesar cipher into themselves, for example "anna" with a shift of 1. And, words can shift to their reverse in shifts other than 13.

There are 25 possible shifts because 14-25 are not reverses of 1-12, all of them are reverses of themselves: Just re-encode the text in the cipher to decode it.

Note that you have to encode them with the Atbash cipher first. If you encode them with the Caesar cipher first, then the Atbash plus Caesar shift is 26 minus the Caesar shift.

9 seems like the cipher with the most pairs, because E and R stay the same, A and I become eachother, and O and U become eachother.

Since this topic has not been explored very much on Word Ways, we decided to include the 4-letter pairs.

Note: There's a dash instead of an arrow because the pairs can go either way in this one.

Here are the 4-letter pairs for each shift, excluding 0:

1-shift -

anan-anan, anna-anna, banc-zany, haji-tars, haps-tali, hasp-tail, hemi-twos, impi-sols, imps-soli, jail-rasp, laps-pali, lwei-pews, mosh-omit, mown-omen, naan-naan, nabs-nazi, nala-napa, nana-nana

2-shift -

ahoy-bund, anan-bobo, anna-boob, hoax-unbe, inby-toad, info-town, inti-toit, jota-snib, knit-roti, muni-phot, node-onyx

3-shift -

ache-cavy, achy-cave, acro-calo, alif-crux, bias-buck, bike-busy, bile-bury, bilk-burs, bill-burr, birr-bull, blog-brow, boas-bock, bobo-bobo, bonk-bops, boob-boob, book-boos, dopy-zone, dunk-zips, durr-zill, gook-woos, howk-vogs, jill-turr, jink-tups, jole-tory, juju-titi, junk-tips, jupe-tiny, jury-tile, kain-scup, kale-scry, kaon-scop, kink-sups, kips-sunk, kirs-sulk, koas-sock, kois-souk, konk-sops, kyak-secs, lias-ruck, lire-ruly, loin-roup, lone-ropy, look-roos, loos-rook, lory-role, lour-roil, luck-rias, lunk-rips, luny-ripe, lyre-rely, mice-quay, neck-pyas, nill-purr, nips-punk, noil-pour, nook-poos, noon-poop, nope-pony, nose-poky, nosy-poke, ogre-owly

4-shift -

apod-dopa, avid-diva, opal-pods

5-shift -

agar-eyen, ajar-even, atma-else, baal-deet, baas-deem, bans-derm, barm-dens, batt-dell, bend-darb, berm-dans, beta-dale, carl-cent, gaen-year, gall-yett, geum-yaks, jane-vera, jarl-vent, late-tela, maar-seen, maes-seam, maim-sews, mair-sewn, male-seta, mall-sett, malm-sets, mana-sere, mane-sera, mara-sene, marl-sent, masa-sume, matt-sell, menu-sark, mesa-same, meta-sale, mung-skry, naes-ream, nala-rete, nema-rase, neuk-raku, neve-rajaa, newb-raid, newt-rail, paan-peer, palm-pets, pans-perm, paua-peke

6-shift -

abbe-feeb, argh-fozy, axon-firs, been-ebbs, boon-errs, born-eros, cobb-dree, coft-dram, cole-drub, colt-drum, jobs-wren, orra-roof, oxen-ribs

7-shift -

agio-gays, agon-gast, agro-gaps, airs-gypo, aits-gyno, byes-fico, coco-eses, hyte-zinc, nips-tyro, ocas-sego, otic-snye, pyro-rips

8-shift -

ahed-hade, atop-hots, buhl-gnaw, chap-fahs, chid-faze, chop-fats, chub-fang, deet-eddo, lahs-whap, lath-whoa, lats-whop, laze-whid, otto-toot, pate-shod, pats-shop, pods-step, pone-stud, pong-stub, pots-stop, pung-snub

9-shift -

axel-ilex, bane-hive, bare-hire, bear-heir, beef-heed, bine-have, boggy-huck, boxy-hulk, bury-hork, bute-hope, cane-give, cape-gite, carp-girt, cavy-gink, cine-gave, cite-gape, coir-guar, crap-grit, crawl-grim, crow-grum, cuif-goad, cure-gore, curt-gorp, dare-fire, davy-fink, deep-feet, dere-fere, dine-fave, diol-faux, dire-fare, dive-fane, dork-fury, dree-free, drip-frat, drum-frow, duck-fogy, dure-fore, jird-zarf, jura-zori, keir-year, made-wife, mane-wive, mare-wire, mark-wiry, mate-wipe, maya-wiki, meet-weep, mere-were, mice-wage, milk-waxy, mine-wave, mink-wavy, mire-ware, mirk-wary, miry-wark, mure-wore, nave-vine, nevi-vena, nite-vape, nixe-vale, papa-titi, pare-tire, pave-tine, perv-tern, pili-taxa, pipe-tate, pixy-talk, pogy-tuck, prat-trip, prau-trio, pree-tree, prep-tret, prey-trek, pure-tore, puri-tora, purr-torr, quit-soap, rage-rice, rape-rite, rate-ripe, read-reif, reed-reef, rove-rune

10-shift -
offs-veer

11-shift -
acta-kirk, acts-kirs, ages-kegs, cees-iggs, cigs-ices, eggs-gees, ekes-gags, etch-grid, mocs-ywis, okes-wags, rows-twos, sacs-skis, sage-skeg, sago-skew, sake-skag, scag-sike, soke-swag

12-shift -
adit-lids, alit-lads, alts-last, arts-lust, aryl-luna, bels-khat, blah-kale, chub-jerk, dahl-ilea, elhi-haed, else-hath, erst-huts, exit-hods, flat-gals, flit-gads, frag-gulf, frat-guls, fuds-grit, peds-whit, pehs-whet, pent-whys, plan-waly, plus-wart, puds-writ, sels-that, serf-thug, shah-tele, slab-talk, slit-tads, surf-trug

13-shift -
beal-limb, beam-lima, bets-litu, byte-loti, city-keto, debt-jilt, deli-jibe, dell-jibb, demy-jiao, difs-jehu, foxy-hypo, nils-zebu, obia-ylem, pout-xyst

14-shift -
anan-nana, anna-naan, azan-nona

15-shift -
alow-odas, back-nome, balk-node, bawk-nose, bobo-nana, bock-name, bolo-nada, bonk-nabe, boob-naan, bozo-napa, bulk-nude, calk-mode, came-mock, chaw-mhos, coco-mama, come-mack, conk-mabe, dame-lock, dank-lobe, dawk-lose, dobe-lank, dock-lame, dome-lack, dunk-lube, edge-klik, fame-jock, folk-jade, funk-jube, glad-idol, hack-home, hade-holk, hame-hock, hawk-hose, sabe-wonk, sock-wame, some-wack

16-shift -
abba-poop, abbe-pool, ally-peer, aped-palm, aper-paly, apex-pals, aryl-pyre, balm-oped, beep-olla, chap-nipa, epee-lall, flaw-kept, flax-keps, flea-kelp, flew-kelt, ghee-jill, glee-jell, help-ilea, hols-ibex, thee-will, them-wild, thew-wilt, till-whee, tilt-whew

17-shift -
bibs-pipy, bids-piny, biff-pill, biog-pick, bits-pixy, diff-nill, dill-niff, dits-nixy, fids-liny, film-life, hill-jiff, iffy-ills, riff-zill, scum-yowe, vids-viny, viff-vill

18-shift -
anon-rede, army-raft, axel-rung, axon-rude, cans-prez, cant-prey, card-prao, cart-pray, dork-odah, dune-oxen, envy-newt, exon-nude, frag-marl, frap-marc, fray-mart, fret-many, grot-lady, hart-kray, inns-jeez, iron-jade, vane-wren

19-shift -
ahed-slop, ahem-slog, alee-shoo, alow-shew, awed-swop, beau-rosy, bedu-ropy, been-roof, beep-rood, bode-repo, boon-reef, bora-rebs, bosh-real, bozo-rete, deal-posh, deed-poop, deep-pood, deme-pogo, dhow-plew, doob-peer, dopa-peds, dosa-peas, dosh-peal, ebbs-orra, elks-ohia, epos-odea, feal-nosh, fogs-nema, food-neep, fora-nebs, geez-moot, goal-mesh, goas-mesa, gobo-mere, gogo-meme, goop-meed, gosh-meal, heed-loop, heme-logo, here-lobo, hero-lobe, homa-legs, hype-ludo, hypo-lude, ikon-kief, ilka-khis, tops-zeda, tory-zebu, tosh-zeal, ween-woof, weep-wood

20-shift -

alga-tint, atap-tate, bats-stab, beta-spat, beth-spam, bile-slip, bite-slap, bits-slab, blab-sits, blam-sith, bleb-sips, clap-rite, clip-rile, clop-rife, glib-nils, ilia-lilt

21-shift -

argh-udon, baba-tutu, back-tusk, bask-tuck, buck-task, bund-tahr, busk-tack, carr-sudd, cask-suck, chao-snug, chat-snub, ciao-smug, cuif-samp, cusk-sack, dusk-rack, fuji-palm, hadj-nurl, hajj-null, hump-naif, juba-latu

22-shift -

arch-veto, arks-veld, avid-vans, bent-uric, bind-unis, bish-undo, chid-tons, chip-tong, cobs-thud, cone-thir, coni-thin, cris-tend, ding-snip, dohs-shod, dona-shiv, dong-ship, dors-shed, errs-reed, ever-rare, evil-rank, ghis-pond, grid-pens, hare-over, herd-ores, ires-nerd, knar-live, kris-lend, when-zori, whir-zone

23-shift -

aide-wots, aims-woke, apod-whit, awed-wast, awls-wale, awol-wail, bids-vote, bise-voes, bobs-vive, boil-viol, boll-vill, bots-vide, bowl-vial, daws-twae, deme-tsks, died-tost, diff-torr, difs-tore, dike-toms, dill-toll, dims-toke, diol-toil, dite-tods, doby-tivy, dodo-titi, dole-tils, doll-till, dols-tile, doms-tike, dorr-tiff, dose-ties, dost-tied, dots-tide, doty-tidy, doum-tick, eche-sups, eide-sots, esse-sees, fibs-rove, fido-roti, fids-rote, fill-roll, fils-role, fits-rode, five-robs, fobs-rive, foes-rise, ford-rift, fore-rifs, fowl-rial, fyce-ryus, heed-psst, hide-pots, hied-post, hies-pose, hike-poms, hili-polo, hill-poll, hims-poke, holopili, hols-pile, holy-pily, homo-piki, homs-pike, hose-pies, host-pied, howe-pias, howl-pial, iced-oust, jive-nobs, joke-nims, jole-nils, jots-nide, kids-mote, kifs-more, kill-moll, kilt-mold, kite-mods, kits-mode, koto-midi, lias-lowe, libs-love, lich-loup, lido-loti, lied-lost, lies-lose, lift-lord, lits-lode, live-lobs, lyes-lyse, lyly-lyly

24-shift -

exit-tape, fete-stet, fixt-spae

25-shift -

call-wynn, crag-whys, duly-vena, fuse-tegu, fuss-tegg, gels-sung, gene-sulu, guff-sett, gulf-sent, hulk-reno, jehu-pure, luff-nett, lulu-nene, mels-mung, meme-mumu, menu-mule, mess-mugg

Some shifts have over 50 pairs like 9 and 23 and 4, 10, 14, and 24 have only 3 or less.

Two 6-shift are connected by a 13-shift cipher: been-ebbs and orra-roof. Some make sense, like kale-blah, ally-peer, and iron-jade. Some are opposites, like junk-tips, and dirge-farce (for 5-letter pairs).

Some go to the reverses of themselves, like avid-diva, stop-pots, and stab-bats.

Some pairs are of one word to the same word, like anna-anna, bobo-bobo, and lyly-lyly.

Some fit into both categories, anna-anna, boob-boob, and naan-naan, which anna, boob, and naan all Caesar shift into each other.

Possibly the best group of multiples are pixy-talk, slab-talk, pixy-bits, and slab-bits.

11 is the champion of words with only odd letters, with 13 out of its 17 pairs having two words with only odd letters (all except acta-kirk, acts-kirs, etch-grid, and rows-twos.)

Some of them make almost sense, like lima-beam(not bean, beam), and mama-coco, the name of a character in the movie Coco (the movie about Day of the Dead, not the Pokemon movie with the same name). Interesting 3-letter pairs include ice-age.

Let's move on to five-letter pairs, surprisingly every shift has at least one pair:

1-shift -

adown-axmen, hajis-tarsi, lalls-pappi, lauan-pagan, limas-psoai

2-shift -

jinny-stood

3-shift -

alias-cruck, aloin-croup, arias-cluck, aryls-clerk, birse-bulky, bloke-brosy, boody-booze, koine-soupy, kroon-sloop, loose-rooky, micas-quack

4-shift -

loppy-spoof

5-shift -

abase-edema, fanum-zerks, inarm-wrens, lemma-tasse, ligam-twyer, maple-septa, miens-swarm, nalar-retem, nasal-remet, natal-relet, pacer-pecan, palet-petal

6-shift -

croon-dorrs, obols-rerun

7-shift -

imago-yugas

8-shift -

chide-fazed, putto-snoot, putts-snoop

9-shift -

barer-hirer, battu-hippo, biker-hayer, biner-haver, caner-giver, citer-gaper, crate-gripe, creep-greet, cripe-grate, darer-firer, direr-farer, dirge-farce, dower-fumer, mater-wiper, miler-waxer, miner-waver, mixer-waler, offer-udder, opera-uteri, otter-upper, pacer-tiger, paper-titer, pawer-timer, piper-tater, poker-tuyer, poppa-tutti, prate-tripe, privy-trank, prune-trove, rater-riper, rawer-rimer

10-shift -

ruffs-speer

11-shift -

sachs-skids, sages-skegs, sagos-skews, sakes-skags, scags-sikes, sokes-swags

12-shift -

adult-liras, bulla-kraal, chert-jehus, elute-harsh, expat-howls, exult-horas, felts-ghost, plasm-waltz, pulse-wrath, rawly-ulpan

13-shift -

celli-kibbe, ditto-jetty, rebbe-villi

14-shift -

fatwa-inurn

15-shift -

boson-nawab, cobia-mango

16-shift -

aptly-pawer, aryls-pyrex, fleer-kelly, tiled-whelm

17-shift -

biffy-pills, bikes-pigmy, biogs-picky, eidos-mincy, hills-jiffy, hilly-jiffs, hippy-jibbs

18-shift -

anode-redon, cajon-pride, carve-prawn, freer-manna

19-shift -

aloof-sheen, bored-rebop, doffs-penna, hoggs-lemma

20-shift -

bathe-stamp, bazoo-stuff, blaze-situp

21-shift -

farms-pudic

22-shift -

cones-third, corer-there, diver-snare, doers-shred, donee-shirr, doves-shard, drear-serve, genic-print, genre-prier, grind-penis, hared-overs, knars-lived, whirs-zoned

23-shift -

apods-white, bouse-vices, dices-touse, didst-toted, diode-toits, diols-toile, ditty-toddy, dolts-tilde, easts-swede, edify-story, elide-slots, elint-slojd, emote-skids, epode-shits, fices-rouse, fiche-roups, fille-rolls, kilty-moldy

24-shift -

fidge-spurt

25-shift -

fella-tunny, gemmy-summa, genoa-sulky, grana-shyly, grunt-shelf, gully-senna, luffa-netty, lyssa-naggy

Most of the 5-letter 9 pairs are the 4-letter ___e -> ___e to ___er -> ____er. The 11 shift also has many pairs of words with only odd-numbered letters (called all-odd words, because "all" and "odd" are also an Atbash plus Caesar shift pair).

The pairs micas-quack and imago-yugas is the longest pair with two all-different-letter all-odd words.

Here are the six letter pairs and longer. All the shifts that have pairs are shown below:

1-shift - banana-zanana

3-shift - booboo-booboo

5-shift - barman-denser, carman-censer, lallan-tetter, mermen-sansar, parser-penman

6-shift - bimbos-extern

8-shift - duende-endued

9-shift - batter-hipper, beader-heifer, believe-hexane, better-hepper, butter-hopper, copper-gutter, crater-griper, dapper-fitter, dipper-fatter, duffer-fodder, jitter-zapper, kipper-yatter, meeter-weeper, nappie-vittae, patter-tipper, peeper-teeter, pepper-tetter, pewter-temper, picric-tagrag, pruner-trover, pumice-towage, putter-topper, rapper-ritter, ratter-ripper, recane-regive, repave-retine, greeter-creeper, gritter-craper, pewterer-temperer

12-shift - furfur-grugru, penile-whydah

16-shift - clover-nebuly

17-shift - ridgils-zinkify

22-shift - corned-theirs, divers-snared, drears-served, incent-nitric, coheirs-thorned

23-shift - holies-pilose, kiddie-mottos, hilloed-pollist

The only seven-letter pairs are greeter-creeper(9), gritter-craper(9), ridgils-zinkify(17), coheirs-thorned(22), and hilloed-pollist(23).

And one eight-letter pair: pewterer-temperer(9).

But we move on to bigger things!

What if we check Merriam Webster's 3rd Unabridged instead of the scrabble dictionary?

We can find 6-letter pairs for most shifts!

For example:

1 - banana-zanana

2 - anatox-bobine

3 - actory-cajole

5 - barman-denser

6 - haboob-yferre

7 - isacco-yogees

8 - duende-endued

9 - pewter-temper

11 - roctas*-twirks*

12 - penile-whydah

13 - divelu-jeribs*

15 - cobola-manado

16 - themer-wildly

17 - dioecy-nicmos

18 - annona-reeder

19 - boreas-rebosa (also an anagram!)

20 - bactra-stract

21 - judaic-larums
22 - divers-snared
23 - kiddie-mottos
25 - felten-tunful

Starred words are inferred words. Judaic, Bobine, Anatox, and Divelu are capitalized words.

4, 10, 14, and 24 are the only missing ones, and starred words are inferred forms not listed but implied.

The 7-letter pairs with this dictionary added are:

3-shift - boobook-booboos

5-shift - attalla-ellette, narayan-reneger

8-shift - shouted-patnode

9-shift - coiture-guapore, crapper-gritter, creeper-greeter, crutter-gropper, elbower-exhumer, otterer-upperer

13-shift - telembi-tibiale

17-shift - ridgils-zinkify

19-shift - alehoof-sholeen

22-shift - conjure-thimber, coheirs-thorned

23-shift - bollies-villose, hilloed-pollist

Also, there are 4 more 8-letter pairs: purupuru-torotoro (shift of 9), hackmack-homecome (shift of 15), conjured-thimbers (shift of 22), hospices-piehouse (shift of 23).

Also, we have a 9-letter shift pair. peneplane-paraptera. I discovered this pair, nobody else may claim that they discovered it.

If you add the words from some more dictionaries, 4 has johppa-upwood and 24 has gjerde-rotgut, only leaving 10 and 14.

Also adding the words from some more dictionaries, there are 2 more 8-letter pairs: balwarra-detienne (shift of 5), and dapperer-fitterer (shift of 9). No new 9-letter pairs other than peneplane-paraptera though.

That is all of the things I currently have here about ciphers and structures. It may be continued in a part 2 with Arithmetic Cipher and Multiplicative Cipher though.