Morthlach Jan 27, 2019 at 3:11pm [genpop44](https://cicada3301.boards.net/user/6) and [a2e7j6ic78h0j](https://cicada3301.boards.net/user/135) like this

Recently there have been questions asked about general methods to check for words when decrypting, here we are not only referring to cipher text decryptions but also words as Keys. A general method is useful because when trying potentially millions of different encryption methods, cribs and keys an automated procedure is required. Other methods, such as [character-n-gram log-probabilities have been described elsewhere.](http://cicada3301.boards.net/thread/36/decrypt-runes-1-basic-tools)  As will be seen, one of the reasons this puzzle is so difficult is the huge space we have to search making only a few assumptions from the solved pages.  
  
Basic Method  
  
In this note we will describe a rune-shift independent method that checks if a ‘candidate’ list of 6 runes is the start of a word. (6 is a reasonable, if we choose too short a number for runes to look for then you get too many spurious hits, much more than 6 results in many words to check.) The candidate could be a decrypted plaintext or keyword. The basic idea is not complicated, but the solved pages introduce a few additional complexities that may also be used in the unsolved pages. If we take them into account then  
  
FIRFUMFERENFE  
  
The key “FIRFUMFERENFE” used in the koan, [“The voice of the I…”](https://docs.google.com/spreadsheets/d/1QsoYQ-NkJcwEuyOgMrD6DkHU2AUktwsfnQGnTURf1bU/edit#gid=1421979231), indicates that any word (especially a keyword) could have one of its letters shifted to “F”.  
  
WIDSOM  
  
This word occurs in the [“Welcome Pilgrim…”](https://docs.google.com/spreadsheets/d/1QsoYQ-NkJcwEuyOgMrD6DkHU2AUktwsfnQGnTURf1bU/edit#gid=2124456769) section of the solved pages. It is assumed to be a deliberate miss-spelling of the word ‘wisdom.’ This causes us many headaches. It means that it is certainly possible that any word anywhere in the remaining text could be slightly miss-spelled. Including all possible typos significantly complicates our search.  
  
Assumptions  
  
It’s always useful to be mindful of our assumptions:  
  
Assumption 0: standard assumptions on [runeglish](http://cicada3301.boards.net/thread/13/runeglish-complete-beginners-introduction), [well-ordering](http://cicada3301.boards.net/thread/37/decrypt-runes-first-pages-solved), etc applies.  
  
Assumption 1: The word we are trying to match has at least 6 runes.  
  
Assumption 2: Those 6 runes are the first runes in the word.  
  
Assumption 3: The word has been encoded in [Forward or Reverse Gematria with any shift.](https://imgur.com/a/D5eBa)  
  
Assumption 4: All occurrences of any letter in the word may have been changed to “F”  
  
Assumption 5: Any two runes next to each other may have swapped positions.  
  
Method  
  
All that is required is a dictionary of runeglish words, [such as here](http://cicada3301.boards.net/thread/36/decrypt-runes-1-basic-tools), and some for loops.  
  
**1.** Take all the words that are 6 runes and longer.  
  
(unique word count = 69957)  
  
  
**2.** Take the first 6 runes of each word, and discard any duplicates. E.g. circumference and circumferences have the same first 6 runes, so only need to be included once.  
  
(unique word count = 26398)  
  
  
**3.** For each word, assume that any of letters could have been shifted to an “F”.  
E.g. ‘FOLLOW’ gives these entries: "FOLLOW", "FOFFOW", "FFLLFW", "FOLLOF"  
  
(unique word count = 167590)  
  
  
**4.**For each word swap any two adjacent runes:  
E.g. ‘FOLLOW’ gives these entries: "FOLLOW", "OFLLOW", "FLOLOW", "FOLLOW", "FOLOLW", "FOLLWO"  
  
(unique word count 787672)  
  
  
**5.**Now we have our complete list of words + possible Fs, plus possible typos, encode them to numbers using the forward and reverse Gematria.  
  
(unique word count 1574860)  
  
  
**6.** Get ‘shift independent’ words by subtracting the first rune’s value of each rune mod 29  
  
(unique word count 1492830)  
  
  
This list is includes: the first 6 runes of all our dictionary words, a possible change of any letter to “F”, a possible typo of two adjacent runes being swapped, forward and reverse Gematria encodings.  
  
To check a candidate word all we have to do is shift it by subtracting the value of the first rune mod 29 from our candidate word and then see if that sequence occurs in the list we just generated. Any 'hits' may be worth investigating further.   
  
One and half million possible words to check against, Isn’t this crazy? Can't we be more smart?  
  
Well, yes, but the puzzle makers deliberately made it that way by including small subtle effects such a typo in the middle of their magnus-opus. Bear in mind this list does not include phrases, what if the key we are looking for is the very reasonable "A KOAN". Well we would have to include our word-n-gram database in the above method, generating untold millions more possibilities. Of course, we are free to cut down our initial dictionary size by removing words, like “aardvark”, that are unlikely to be in the Liber Primus … This is about the most justifiable method to reduce the number of search words. [Some initial attempts were described here.](http://cicada3301.boards.net/thread/46/words-liber-primus) We could also assume they never make another typo, or that only consonants are shifted to F etc. ...   
  
Final Thoughts  
  
As we have seen here and in many other examples, using very general methods in this puzzle leads to countless millions of possibilities. Trying to cut that space down requires making assumptions that may or may not be true. If it is possible to decrypt the runes with just the rune-information on the the unsolved pages then we are searching for a needle in a giant haystack.  
  
  
\*Comments, questions, suggestions, omissions etc ? please try [#cicadasolvers](http://webchat.freenode.net/?channels=cicadasolvers)