Today we are studying doubling and halving.

1. Which number and letter do you get by doubling:

b = 1?

c = 2?

d = 3?

(What happens if the number gets too big?)

n = 11?

t = 16?

z = 21?

y = 20?

2. How do we do the reverse? What letter and number is sent to these letters by doubling?

C = 2?

F = 4?

H = 6?

(What happens if the number is odd?)

B = 1?

D = 3?

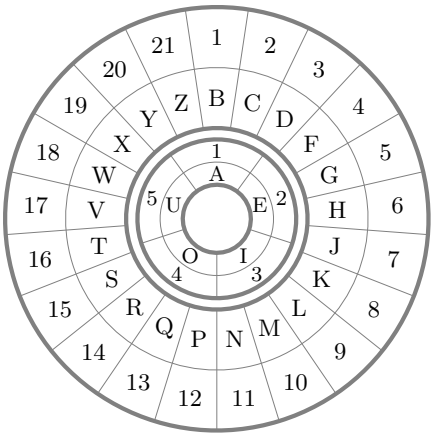
X = 19?

3. If you don't mind negative numbers, sometimes they help with big numbers.

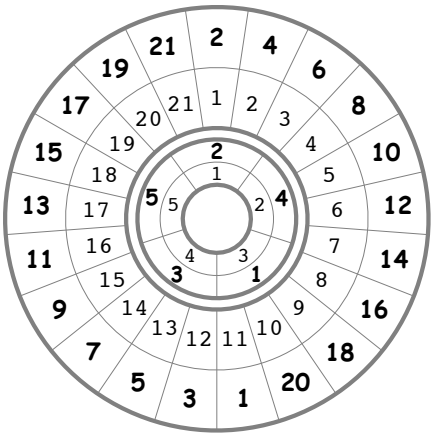
19-21 = -2, what is half of -2? what letter is -1?

The left wheel converts letters to numbers normally. The middle wheel doubles numbers. The right wheel has the numbers replaced by letters.

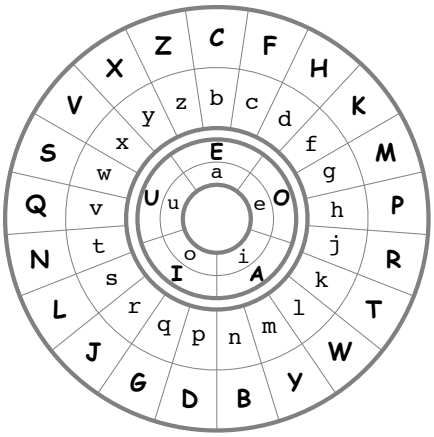
Letters to numbers
(nothing new)



Encrypt numbers
(`inner` rings to OUTER)



Encrypt letters
(`inner` to OUTER)



Let's look at how to find the key, cryptanalysis.

1. Name three things that are messed up when converting `plaintext` to CIPHERTEXT using the shift cipher and the double cipher.

2. Name two or three things that are preserved from `plaintext` to CIPHERTEXT using the shift cipher and the double cipher.

3. Name one thing that is preserved by shift but not by the double.

Hint: The word `double` cannot be taken to `hiucwo` by a shift cipher, because the vowels in `dOUble` are different than in `hIUcwo` .

4. Name one thing that is preserved by double but not by shift.

5. What are some letters, syllables, words or fragments that are common in English that can be found in the ciphertext without knowing the key?

6. Decrypt the shift cipher message **Ap drubu ac o leet drod jei goxd de buon, lid ad rocx'd luux gbaddux jud, jei wicd lu dru exu de gbadu ad.**

Hints: (a) What is the 4th word? (b) What are all the vowels? (c) From #3 what do you guess about JEI or WICD ? (d) What are all the consonants?

English data - here are some statistical observations about "English" by Barry Keating at Notre Dame. The most common:

single letters: E T A O I N S H R D L U

one-letter words: a I

first letters: T O A W B C D S F M R H I Y E G L N P U J K

last letters: E S T D N R Y F L O G H A K M P U W

pairs of letters: th er on an re he in ed nd ha at en es of or nt ea ti to it st io le is ou ar as de rt ve

two letter words: of, to, in, it, is, be, as, at, so, we, he, by, or, on, do, if, me, my, up, an, go, no, us, am

triples of letters: the and tha ent ion tio for nde has nce edt tis oft sth men

three-letter words: the, and, for, are, but, not, you, all, any, can, had, her, was, one, our, out, day, get, has, him, his, how, man, new, now, old, see, two, way, who, boy, did, its, let, put, say, she, too, use

four-letter words: that, with, have, this, will, your, from, they, know, want, been, good, much, some, time

Be careful: be sure to use data for the language in use, which depends on who is speaking and over what medium