Today we are studying doubling and halving.

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

b = 1? 1+1 = 2 C

c = 2? 2+2 = 4 F

d = 3? 3+3 = 6 H

(What happens if the number gets too big?)

n = 11? 11+11 = 22 = 21+1 B

t = 16? 16+16 = 32, 32-21 = 11 N

z = 21? 21+21 = 42, 42-21 = 21 Z

y = 20? 20+20 = 40, 40-21 = 19 X

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

C = 2? b = 1

F = 4? c = 2

H = 6? d = 3

Just Look in reverse

Also easy to divide even number by two

(What happens if the number is odd?)

B = 1? B = 21+1 = 22, 22/2 = 11 n

D = 3? D = 21+3 = 24, 24/2 = 12 p

X = 19? X = 19+21 = 40 40/2 = 20 y

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

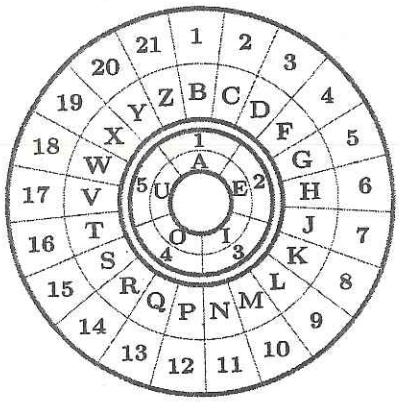
19-21 = -2, what is half of -2? what letter is -1?

↑ −1 −1+21 = 20 y

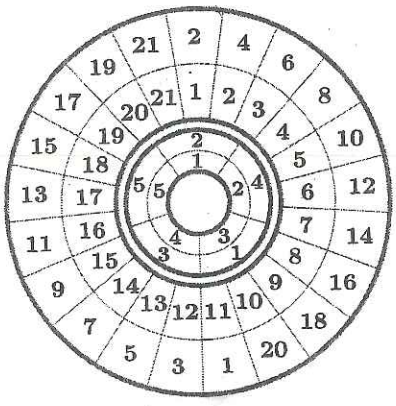
same answer

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

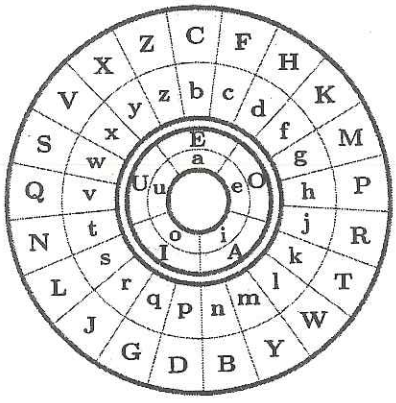
Letters to numbers (nothing new)



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.

The letters change ... (I don't think anyone gave a different answer)

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

Vowels vs Consonants. If P goes to C once, then it does every time. # of letters, vowels, consonants, words

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

Distance between letters. So "BD" is probably "rt" ← (skip one)

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

U → U, Z → Z some letters don't change!

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?

"rt" in shift, just look for two letters that skip one, like BD, CF, ~~FH~~, GJ, etc.
Single letter words: I or a

6. Decrypt the shift cipher message **VJI GEAMV, FIES CSAVAT, OT PUV OP UAS TVEST, CAV OP UASTIMWIT, VJEV XI ESI APFISMOPHT**

HOMEWORK (feel free to work in groups)

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