

MA111: Contemporary mathematics

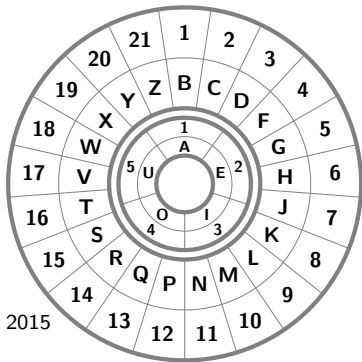
Entrance Slip (due 5 min past the hour):

Use a shift of 5 (so that $d=3$ becomes $K=8$) to encrypt the message:

“this quiz is too easy”

Schedule:

- HW 1 is due Tuesday, Oct 6th, 2015
- Mini-Exam 2 is in-class on Thursday, Oct 8th, 2015
- HW 2 is due Tuesday, Oct 13th, 2015
- HW 3 is due Thursday, Oct 15th, 2015
- HW 4 is due Tuesday, Oct 20th, 2015
- Exam 2 is in-class on Thursday, Oct 22nd, 2015



Today we use numbers to make using the codes easier.

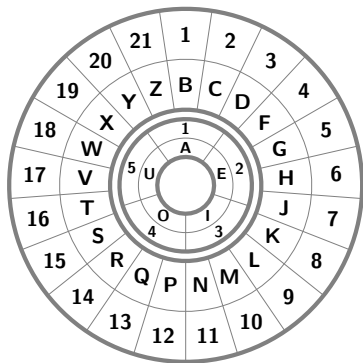
While we are passing out the worksheet...

- Please turn in your entrance slips.

Use a shift of 5 (so that $d=3$ becomes $L=8$) to encrypt the message:

“this quiz is too easy”

- What is $16 + 5$?
- Where does $t=16$ go? $Z=21$
- What about $20 + 5$? Where does $y=20$ go?
- Is there a simpler way of describing the vowel shift?
- What about a shift of 10? What about 11?



Old words

- General words

plaintext (plain message, “can you keep a secret”)

ciphertext (hidden version, “DEP ZUA LIIQ E TIDSIV”)

encryption (how to convert plaintext to ciphertext)

decryption (the reverse, cipher to plain)

cipher (both encryption and decryption methods)

key (a small secret that lets you change the cipher)

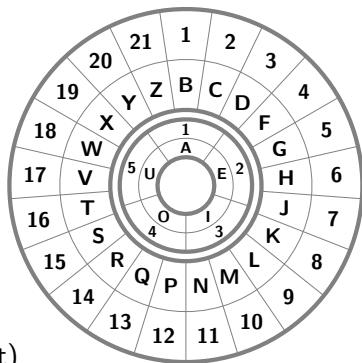
- Shift cipher

Encrypt: shift vowels and consonants right by an amount according to the key

Decrypt: shift vowels and consonants left by an amount according to the key

New words: shift cipher with numbers

- To encrypt with shift cipher, add the key to the number, using wrap-around if too big (subtract 5 if a vowel, or subtract 21 if a consonant)
- To decrypt with shift cipher, subtract the key from the number, using wrap-around if too small, (add 5 if a vowel, or add 21 if a consonant)
- For example if the shift key is 7, then $g=5 \rightarrow P=12$, since $5 + 7 = 12$ and $w=18 \rightarrow F=4$, since $18 + 7 = 25$ and $25 - 21 = 4$.
- And to decrypt,
 $P=12 \rightarrow g=5$, since $12 - 7 = 5$ and
 $F=4 \rightarrow w=18$, since $4 - 7 = -3$ and $-3 + 21 = 18$.



New words: double-it cipher

- The double-it cipher has no key (we'll fix that next week).
- To encrypt, double the number using wrap-around.
- To decrypt, ...fill in the decoder wheel? (we'll find a faster way next week)

Exit quiz

- Decode this message knowing that it is encoded using a shift cipher that takes b to P
- “Kvifi ror hvi ebozeyg tu?”

