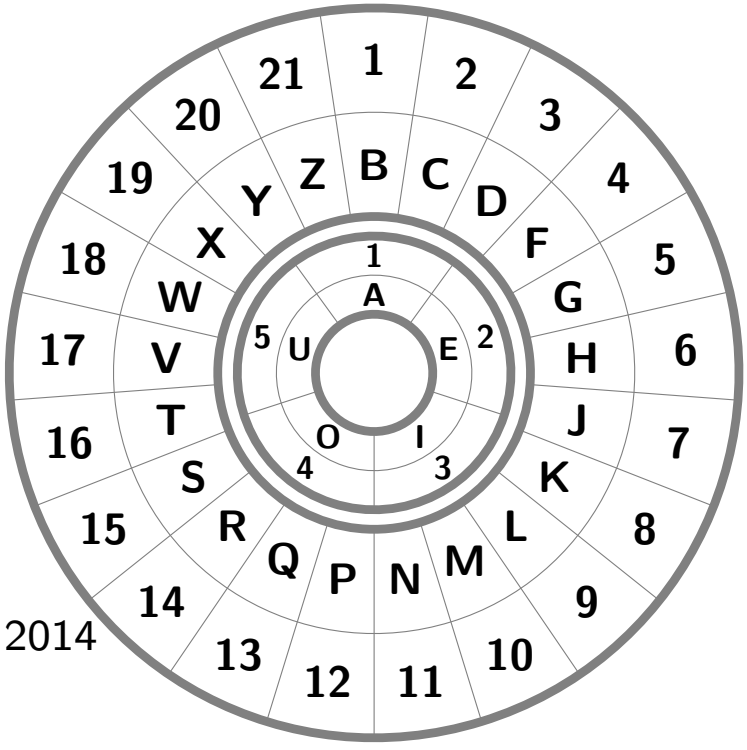
MA111: Contemporary mathematics

Entrance Slip (due 5 min past the hour):

What key is used to shift **`feedback`** to **`KOOHCEFT`**? What is going on?



Schedule:

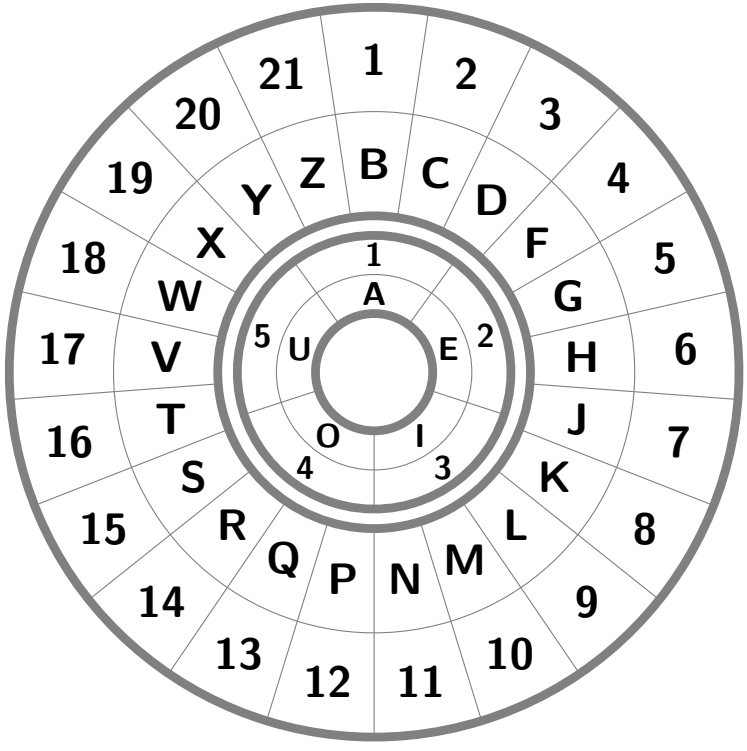
- HW 1 is due 10am Thursday, Oct 9th, 2014
- Mini-Exam 2 is in-class on Thursday, Oct 9th, 2014
- HW 2 is due 7am Wednesday, Oct 15th, 2014
- HW 3 is due 7am Wednesday, Oct 22nd, 2014
- Exam 2 is in-class on Thursday, Oct 23rd, 2014

Today we use numbers to make a new cipher.

While we are passing out the worksheet...

- Please turn in your entrance slips. We will do this every non-exam day.

  Please bring your own 3x5 index cards.



- Might be easier to use numbers:

  feedback 4,2,2,3,1,1,2,8

  ↓ ↓

  KOOHCEFT 8,4,4,6,2,2,4,16

- If we rearrange we get:

  bcdfkae 1,2,3,4,8,1,2

  ↓ ↓

  CFHKTEO 2,4,6,8,16,2,4

- What is going on?

Old 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)

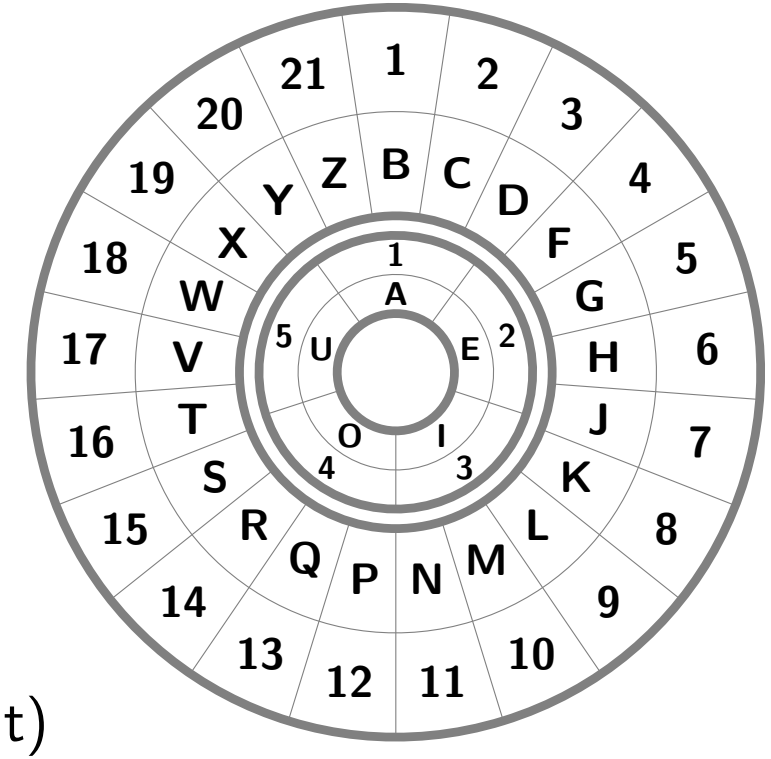
cipher (both encryption and decryption methods)

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

numbers (are used to represent consonants and vowels)

shift cipher (use addition and subtraction with wrap around)

New words: double-it cipher



- To encrypt with double-it cipher,
  double the number,
  using wrap-around if too big
  (subtract 5 if a vowel, or
  subtract 21 if a consonant)
- To decrypt with double-it cipher,
  divide the number by two,
  using wrap-around if odd,
  (add 5 if a vowel, or add 21 if a consonant)
- To encrypt,
  g$= 5 \rightarrow$ **M**$=10$, since $5 + 5 = 10$ and
  w$=18 \rightarrow$ **S**$=15$, since $18 + 18 = 36$ and $36 - 21 = 15$.
- And to decrypt,
  M$=10 \rightarrow$ **G**$= 5$, since $10/2 = 5$ and
  S$=15 \rightarrow$ **W**$=18$, since $36/2 = 18$ and $15 + 21 = 36$.

New words

- **Cryptanalysis** is the study of ciphers, usually with the intention of easily encrypting or decrypting without the key, or easily finding the key
- We almost always assume you know which cipher is in use, but not what key
- **Frequency analysis** - you know some **`CIPHERTEXT`** and what language the **`plaintext`** came from, but not exactly what the plaintext is.
- **Known-plaintext** - you know a little **`plaintext`** and the **`CIPHERTEXT`** it encrypts to.
- These are the main ones we can do on the exam

Optional new words

- Here are some other situations:
- **Brute-force** - just try all keys (takes too long on an exam)
- **Chosen-plaintext** - you get to choose **`plaintext`** and they tell you what it encrypts to

  Surprisingly it is often possible to trick someone into encrypting a few messages for you

  Send someone a text and wait for an encrypted message of the right length to show up

Optional new words

- **Chosen-ciphertext** - you get to choose **`CIPHERTEXT`** and they tell you what it decrypts to

  More surprisingly it is often possible to trick someone into decrypting a few messages for you

  In real life, one sends garbage to a wireless router and looks at the error message to see what part it didn't like

- **Side-channel** - you watch the person encrypting or decrypting in a chosen-whatever situation, and based on how long they take to do it you get more information

  This is a popular modern mechanism. For us, you might ask them to encrypt **`bdlty`** and see which letter is the first one that takes a long time. That is probably the first time it wraps around.

Exit quiz

- Decrypt this message knowing that it is encrypted with the double-it cipher:

- "**`WATO E CILL`**"