Caesar and Atbash

2/21/21

Google Classroom

Intro: https://classroom.google.com/c/MjYzNjg5OTU4MDE5?cjc=6d6lap4

Code: **6d6lap4**

Advanced: https://classroom.google.com/c/MjY0Mzc4MDMwMDE1?cjc=jtxqgrx

Code: jtxqgrx

This is where I'll post resources + any homework we might have

Looking Ahead

(4) Affine & Vigenere

Baconian - Pollux & Morbit

Rail Fence - Patristocrat

Xenocrypt - Hill & RSA*

Review (11)

*Div C ciphers, but if you want the head start I'll teach them

The Alphabet as Numbers

The majority of codebusters involves the use of math to encode and decode messages

How many letters are there in the alphabet? (Zoom quiz)

Yep, 26. For codebusters purposes, we're going to assign 0 to A, 1 to B, and so on until we get 25 = Z.

Getting fast at letter-number conversions is essential

https://quizlet.com/393552971/codebusters-letters-to-numbers-flash-cards/

Put this Quizlet I made on Write mode or however you learn best

- Eventually, conversions will be effortless and take less than a second

Some tips for memorizing letter-number conversions

Choose anchor points - it can be hard to memorize all of the conversions, but if you memorize enough landmarks it will be easy to count from them

- For example: say I memorize that I = 8. If I need to convert L to a number, I can say the alphabet in my head (H I J K L), realize that L is 3 letters after I, and find that L = 8 + 3 = 11.
- Good anchor points: **A=0** (bc easy), **E=4** (bc E is super common), **I=8** (in general just memorize the vowels), **O=14** (vowel), **T=19** (common), **Z=25** (easy)

*This is just how you should start off. Eventually, full mem

is kinda necessary

Caesar Cipher

Basically an Aristocrat, but with a catch

- Letters are not randomly substituted, but have a pattern of addition instead
- “Encode with a Caesar shift of 6” means add 6 to each letter.
  - “HELLO” (7,4,11,11,14) encodes to “NKRRU” (13,10,17,17,20)
- When you encode, you add. When you decode, you subtract.
- “This Caesar cipher has been shifted 8 places. Please decode it.”
  - “WWXAQM” (22,22,23,0,16,12) becomes “OOPSIE” (14,14,15,18,8,4)
- One annoying thing about Caesars and Atbashes is that frequency tables usually aren’t given

Intricacies of Caesar

“What happens if I add and get a number above 25?”

- This would happen during **encryption**. If you get a number larger than 25, **take it mod 26**. In other words (in our limited scope), subtract 26.
  - Ex: 34 would become 34 - 26 = 8, which converts to **I**
  - Mod (modulo) 26 actually means you divide by 26 and find the remainder, but subtraction is fine for our purposes

“What happens if I subtract and get a negative number?”

- This would happen during **decryption**. Do the same thing as before, but in the opposite direction: **add 26**.
  - -8 would become -8 + 26 = 18, which converts to **S**

Strategies for encoding/decoding Caesar

Encoding:

- Do only 1 addition problem for each unique letter, and fill in all of them
  - Ex: If you are encoding by a shift of 5 and there are 11 N's in the quote, do 13 + 5 = 18 = S only once and fill in S for N all 11 times in the quote.

Decoding:

- You can just solve it like a regular aristocrat, only now you can check your work by making sure that the subtraction is consistent.
- Or you can brute-force subtract the entire thing

Caesar Encode Example (just math)

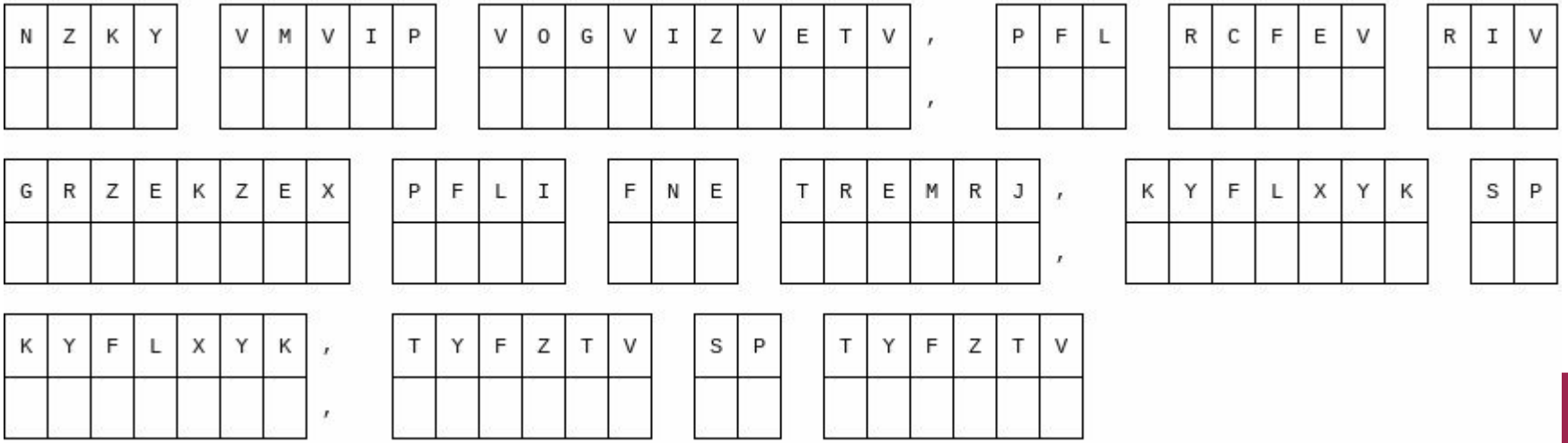
Encrypt these lyrics with a shift of 5.

ALL I DO IS WIN WIN WIN NO MATTER WHAT



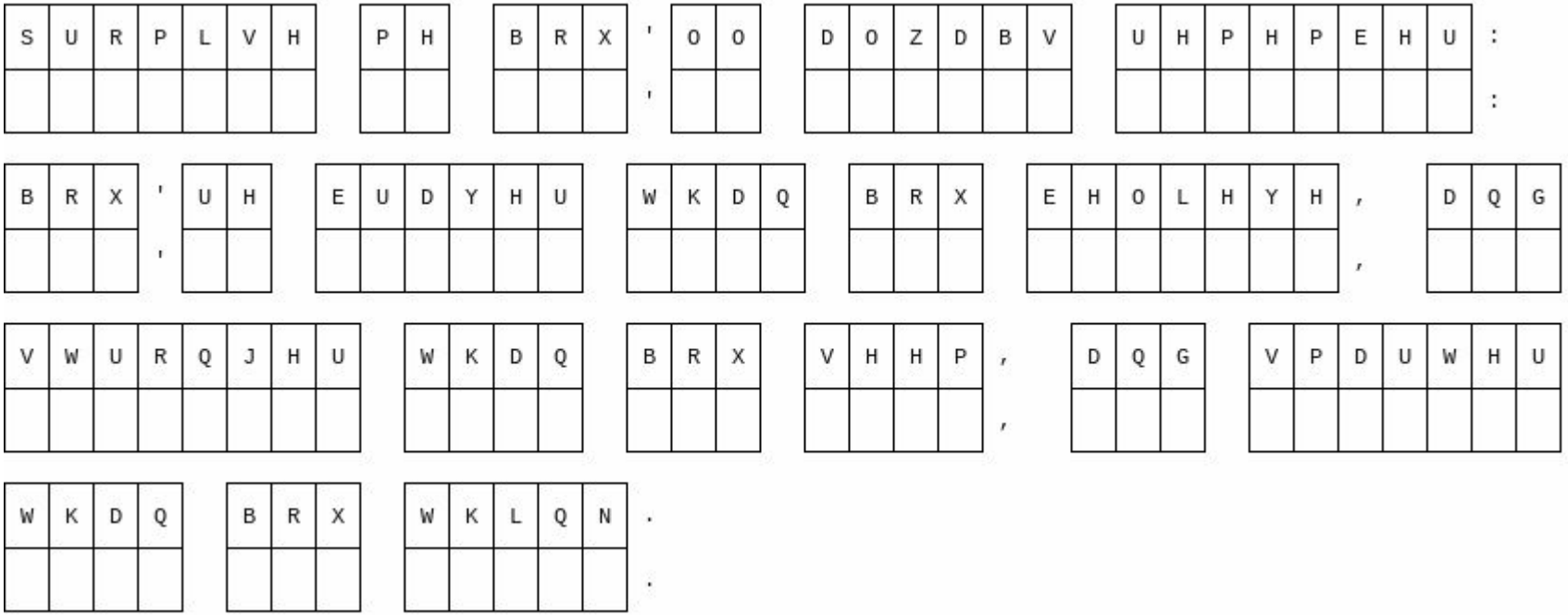
Caesar Decode Example (just math)

Decode this message that has been shifted 17 places.



Caesar Decode Example (like an aristocrat)

Decode the Caesar cipher (notice how it doesn't tell you the shift).



Atbash Cipher

Uses the concept of letter-number conversions as well

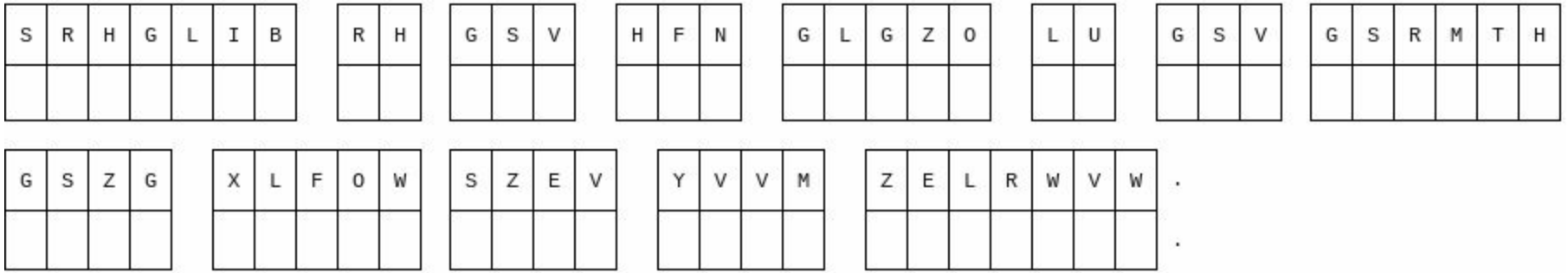
Pretty sure you only have to decrypt, but decoding is the same as encoding for this

To decrypt: substitute in the “complementary” letter (a term I made up)

- Like how complementary angles in a triangle add up to 90 degrees, complementary letters add up to 25 (ex: A and Z are complementary, so are B and Y).
- ZKKOV KRV decrypts to APPLE PIE

Alternatively, just solve like you would do an Aristocrat (because it’s still 1-to-1 letter substitution)

Atbash Practice



Up Next

Keep practicing on Puzzle Baron's Cryptograms

I'll post a new homework json for this week on Google classroom

- Make sure to check out the video I posted last week on how to use Toebes

Vigenere & Affine scheduled for next lesson if you want to take a look ahead

