

Project 1 Work Log

Group: Sid Udata, Shrey Mehta, Shiven Sasipalli

Using this Ed post as a reference

Note: We kept each of our cyphers as separate functions. Each has an encoder and decoder that also started as separate functions so that we could keep track of them without having to worry about code getting messed up with pulling and pushing the master function, which we compiled in the last few days.

March 6

Group meeting - 2 hrs

- Discussed the topic of our project
- Decided on different types of ciphers
- Inspired by "Codebusters" in Science Olympiad

March 7

Group meeting - 1 hr

- Finalized proposal for submission
- Decided on 3 ciphers: Caesar, Vigenere, Hill (each differ in critical ways, compelling us to use different techniques we learned so far)

March 8

Group class time - 1 hr

- Began to pseudo-code our different ciphers (making sure that we fully understand how these ciphers work!)

Sid solo time - 1.5 hr

- Started master let2num function

Shrey solo time - 1 hr

- Set up the code framework/logic

Shiven Solo Time - 1 hr

- Researched how the Hill cipher is encoded and decoded

March 9

Sid solo time - 1 hr

- Finished master let2num function

March 10

Group class time - 1 hr

March 11

Sid solo time - 1 hr

- Started and finished num2let functions

Shrey solo time - 2 hr

- Started the Vigenere shift encryption
- Checked and compared the size of inputted message and keyword (this is important for the Vigenere shift to work, it's not as simple as a mononumerical shift.)

Shiven Solo Time - 2 hr

- Planned out approach for encryption and decryption code, including what steps to take in what order and what variables and inputs would be needed

March 12

Sid solo time - 1 hr

- Started Caesar encoders
- Still uses a fixed shift, but it's good for manually checking if the shifting is working

Shrey solo time - 2 hr

- As per the "mechanism" of a Vigenere cipher, created matrices of different dimensions and elements based on the sizes of the keyword and message (very unique step to this particular cipher)

Shiven Solo Time - 2hr

- Tested matrix multiplication code to make sure it was properly working

- Ended up finding about the `mtimes()` function and implemented that to make sure it worked properly

March 13

Group class time - 1 hr

March 14

Sid solo time - 1.5 hrs

- Issue: `let2num` and `num2let` don't account for lowercase letters
- Added "space" to `let2num` and `num2let`
 - Still issues, with "space" being treated the same as "a"

Shrey solo time - 3 hrs

- Figured out how to properly conduct the "shift" using the keyword (created `letter2numMessage` and `letter2numKeyword`, which then led to the resultant vector, `numbersShiftedvec`)

Shiven Solo Time - 1.5 hr

- Worked on making the inverse matrix code and researched extended Euclidean algorithm

March 15

Group class time - 1 hr

- Fixed `let2num` and `num2let` issues with "space and "a" confusion
- We can now use them for all the other ciphers

March 16

Sid solo time - 2 hrs

- Finished Caesar encoder
- Caesar encoder successfully converts the message from letters to numbers, including spaces. Shift is now random, instead of fixed.

Shrey solo time - 2 hrs

- Ran into some issues with edge cases → what if the resultant vector included a number that was greater than 26, and therefore, not a part of the alphabet?
- Fixed this issue by created another *for* loop that checks each element of the resultant vector and uses the *mod* function to start the alphabet once again after 26 is reached

Shiven Solo Time - 1.5 hr

- Continued researching extended Euclidean algorithm and how I could implement it into determining inverse matrix, ended up finding out that Science Olympiad gives predetermined equivalences that we can use

March 17

Group class time - 1 hr

- Started to think about what to do with spaces in the Vigenere cipher → the encoder code was not working when the inputted message contained a space (ex. HI SHREY)

March 18

Sid solo time - 1 hrs

- Made *let2num*, *num2let*, and Caesar encoder work for lowercase letters
- Used to only be uppercase letters

Shrey solo time - 2 hrs

- Tried to find different ways to fix the “spaces” issue → ultimately decided that it would be best to remove the spaces in the original message and treat the input as a continuous sequence of letters! This fixed up the issue.

Shiven Solo Time - 2 hr

- Did all of the encryption code

March 19

Sid solo time - 2.5 hrs

- Started Caesar decoder
- Issues with the shift just outputting a vector of the correct length but all values are the same, e.g. [23 23 23 23 23 ...]

- Other issues - shift outputs only ascending values?? E.g. [1 2 3 4 5 ... 27 1 2]

Shrey solo time - 2.5 hrs

- Started the Vigenere decrypter (very similar logic to the encoder, but this time, I would be subtracting the shift from the inputted message rather than adding!)

March 20

Group class time - 1 hr

- Debriefed on each other's progress – Caesar and Vigenere encoders are complete.

March 21

Sid solo time - 2 hrs

- Finished Caesar decoder
- Added Caesar encoder and decoder to master script
- Edited prompts into master script

Shiven Solo Time - 1 hr

- Planned out the code for matrix multiplication and implemented

March 22

Sid solo time - 2.5 hrs

- Combined Caesar and Vigenere ciphers into master script

March 23

Sid solo time - 1.5 hrs

- Added comments to Caesar encoder and decoder
- Added Hill cypher to master script

Shrey solo time - 3 hrs

- Finished the Vigenere decoder! Extremely similar to the encoder like mentioned before.
- Decided to stay consistent regarding the spaces → the result decoded message will assume that the inputted encrypted message has no spaces!

Shiven - 6 hrs

- Did thorough testing with different key words to ensure that program was fully functions, provided inputs were given within useable parameters
- Commented on the code to ensure it is readable

March 24

Group - 2.5 hrs

- Finished video submission (includes running of the code and explanations)
- Uploaded and submitted final project