Project Plan

Overview:

Our goal is to create a teaching/learning aid for Professor Joe Li to use in his class on cryptography. This tool will be able to visualize the steps necessary to encrypt and decrypt text using the Vigenere cipher by animating the steps of the encryption process. The user will be able to control the speed as well as step through the steps manually. This system was designed to be used in class as a 88888 as well as something a student could use at home for more exploration.

Structure and Communication:

Our team lead is Joshua Fawcett, though as a small team decisions will be made as a group.

Tasks will be assigned to all group members either individually or as pairs. These assignments will be recorded along with their completion dates within a google spreadsheet document that all team members have editing privileges for.

Task completion will be reported to and confirmed by at least one other member of the team, preferably the team lead.

Our team will meet at least twice a week:

- Tuesdays @ 12:00 PM
- Fridays @ 3:00 PM
- Extra meetings to be scheduled as needed

The team will meet via zoom so that we can talk face to face and collaborate on implementations and problem solving. Day to day communication and general updates will be handled through a discord server where team members can talk via instant messaging and voice chat channels as needed.

Tuesday and Thursday scheduled meetings will have a mandatory attendance while extra meetings will not though all members who can are expected to participate. Team members will report on the completion of their assigned tasks either before or during a scheduled meeting so that other team members can confirm and double check their work.

The individual modules and codes will be kept on a GitHub repository where all team members can access all parts. Any and all edits will be recorded by GitHub at the time of the edit, including adding and removing items from the repository.

Tentative Build Plan:

1. Interviewing Professor Joe Li (5/06)
2. Research
    a. Visualization tools
    b. Existing research on algorithm visualization

    c. Existing software
3. Cipher functionality
    a. Encryption/ Decryption
4. Visualizations
    a. Pacing tool
5. User interface
    a. Executable file
6. Instructions/ Information
    a. Using the tool
    b. Cipher informaion
7. Additional functions if time allows
    a. Cryptanalysis (breaking the cipher)
    b. Knowledge check and testing

Build Plan Rationale:

We will start with researching various articles on algorithm visualization and existing cipher visualization tools in order to assist us in the process of creating requirements and designing our system. Then we will get started with the basic functionality of the system, with each of the separate modules being created in parallel by separate group members. This will allow us to make progress quickly towards creating an initial prototype. Our initial implementation of the system will include only the essential features such as cipher functionality (encryption/decryption), cipher visualization, and the user interface. After developing a working initial prototype then we will revise our system and add some secondary features.

(1) Initially Meghan and Yuyao looked into what library or coding system that would best suit the needs of an interactive animation of the cipher while Max and Josh looked into more specific requirements for a teaching and learning tool. (2) The work was then split depending on proclivity and knowledge, Max working on the base game functionality and Meghan helping and building some sub menus and buttons. Josh built the algorithms then assisted Yuyao with the visualization/animation. (3) The individual pieces were then brought together and bug tested. Menu buttons were mapped to the correct menus, control buttons were given functionality and extra information was added for the user.

Risks:

1. Expected
    a. Lack of knowledge
    b. Poor communication
    c. Delayed assigned tasks
    d. Time restraints

2. Unexpected
    a. Emergencies (medical, family, natural disasters)
    b. Hardware/ software malfunctions (computer breaks, internet goes down, etc.)
    c. Other unforeseen problems

1.

(a) No one was expected to know what the specific requirements of the system were going to be and as such no one was expected to know how best to meet those requirements.

We all needed to learn:

-Who this system would benefit

We contacted Prof. Joe Li who teaches the applied cryptology class and interviewed him on the necessities of his class and the type of system that he could use.

-User requirements

We got initial requirements from Prof. Joe Li during the interview, we also met with him a second time to show our progress and see if there was anything that was missing. We also did some research about algorithm visualization as a learning tool to get other requirements.

-Pygame

We found a book about the library and as a popular game maker there was a lot of other information, tutorials, and examples to be found online.

-The Vigenere cipher

We talked to Prof. Joe Li as well as researched about this particular cipher.

(b) Communication is difficult during a pandemic where all communication needed to be through a computer screen and not in person. We worked on keeping each other updated as we worked on and completed tasks. We asked for help when necessary and met via zoom and saw each other face to face at least twice a week. We also kept meeting notes (see below) and an active spreadsheet of assigned tasks and other project requirements that were constantly updated and could be referred to as needed.

(c) Any tasks that were part of the critical path (see the Gantt chart below) needed to be completed in an orderly and timely fashion. If there were delays in these necessary components we worked together to ensure the delay was as minimal as possible and we could still complete the system ontime.

(d) As students we all had other classwork as well as jobs and other demands of our time. Unexpected emergencies could also limit the amount of time a particular team member might have to work on the system as well. We worked around this by being flexible with what was assigned to whom and worked together to assist each other when due dates were coming up.

2.

With all unexpected risks there is no one correct way to plan for and prevent them. They can all be worked around with flexibility and understanding by the team as a whole. Some emergencies are unavoidable and happen too fast to predict, others can be seen coming and can be mitigated. Not everyone can have reliable setups but we all know there are computers available at school and we kept our documentation, notes, code, and other shared materials on various servers accessible by everyone (Discord, GitHub, Google Drive). While some personal progress might be lost the project as a whole would not be.

Meeting Notes

Last Updated: 5/31/2021

These will be the meeting notes for our meetings, and the unique topics that pertain to those meetings. Joshua will lead the meetings but we will take turns on taking notes during meetings. We will start with Max, and rotate down the group members alphabetically by last name. Josh is exempt from notes in order to focus on leading meetings.

The notes will follow the general format of:

- Date, attendance, time
- Topics to discuss and whether or not they were, indicated by a check mark
- General notes (bugs, additions, ideas, thoughts)
- Individual progress (what was worked on, what is next, what is holding you back)

Meeting Notes for 5/28/21 at 3:00

Attendance: all
3:00 - 3:50

Topics to discuss

_v_ Progress and next steps

Notes:

- Change color of pause to red when activated, color of play to green when activated
- Add one button for pause/play
- Add indicator for what speed you are on
- Split button into visualization and testing (if time permits)
- Error message on screen
- Format buttons correctly
- Limit input (prevent overlap with letters and table)
- Fix issue with screen being black when changing screen size while animation is paused

Max - Not too much progress since last meeting. Next: menus set up (all buttons between menus) (use menu, …), Holding Back: Nothing of note

Josh - Integrated table into the main program. Added pacing functionality (pause/play, step forward/back, speed up/down, restart). Next: Help with other tasks. Holding back: No

Yuyao - Not too much progress since last meeting. Next: Print current message, keyword, and result to screen and implement highlighting specific letters. Possibly help with other tasks. Holding Back: No

Meghan - Not too much progress since last meeting. Got some stuff typed up. Next: get it into the scene manager. Holding back:

Meeting Notes for 5/26/21 at 3:45 - Meeting with Prof. Joe Li

Attendance: all + Professor Joe Li
3:50 - 5:00

Topics to discuss
_√_ Talk about prototype
_√_ Get feedback from professor Li
_√_ Progress and next steps

Notes:
To make better:

- indicate which line is ciphertext, which is key (Label what is what)
- more descriptions, which color is for what
- Describe which process is currently being shown
- One more thing to suggest: Vernam cipher (1 time pad? 1 time pass?) (if time permits), if done in time can possibly show in next class for applied cryptography,

Max - work on next: Work on some more menus and integration between the scenes

Josh - update pacing, using values from encrypt/decrypt to dynamically highlight correct values

Yuyao - Animation, cipher/table integration

Meghan - Info write up and formatting, project plan paperwork

Meeting Notes for 5/25/21 at 12:00 - Group Meeting

Attendance: all
11:45 - 1:00

Topics to discuss
_√_ Check up on everyone's progress

Notes:
Josh - worked on pacing and visualization highlighting. Next: work on integration

Meghan - buttons for animation scenes, work on pausing game

Yuyao- Made letter grid, looked at highlighting stuff, Next: focus on animation, not sure what next task is, focus on integration

Max - Worked on changing between menus, and

Meeting Notes for 5/21/21 at 3:00 - Group Meeting

Attendance: Max Hopkins, Meghan Riehl, Yuyao Zhuge

Topics to discuss
_v_ Check up on everyone's progress

Notes:

- Don't use a slider for speed, use buttons.
- Speed up/speed down buttons will display a number on the screen showing your speed.
- Need step forward and step back as well.
- Main menu will have input/start buttons, it will load the visualization menu.
- Josh could help Meghan with her next task over the weekend.
- Possibly CC Hornof to the prototype meeting.
- Need to have a prototype done by 5/24, some slack time for a meeting on Wednesday.
- Send an email to Joe Li by Monday.

Josh: Worked on: Created Cipher.py with basic encrypt/decrypt functionality. Started basic research about pygame to help with understanding of each module. Next: update Cipher.py? Maybe help implement other modules? Holding Back: Not sure what I need to do next, waiting for progress on other parts to see how Cipher.py might need to be modified, or if there are other parts of the project that I need to help with.

Meghan:worked on: Pseudo code, learning pygame. Next task: add mouse logic/buttons for the speed up/speed down buttons. Holding back: TIME.

Yuyao: Worked on table/grid. Next task: Update table to include letters and highlighting. Holding back: Time.

Max:worked on: Setup test menu/learn pygame. Next task: Setup the main menu to have inputs and load the next screens. Holding back: Other assignments/time.

Meeting Notes for 5/18/21 at 12:00 - Group Meeting

All in attendance
11:45 - 12:20:

Topics to discuss

_√_ pygame yes or no? Yes

_√_ Talk about individual progress

- What are your responsibilities on the project?
- What have you done in the last few days?
- What is your next task?
- What, if anything, is holding you up from accomplishing that task?

_√_ Discuss system building plan (What you'll build and how you'll build it)

Notes:

-Max's research: important to control pacing, being able to rewind, hypertext.
-If not using a flask server: how will we handle user inputs? PyGame has options to build an interactive menu.
-How could we best deliver the final product to Prof. Joe Li? Ask him
-Find and try games built by pyGame to test/learn how it works from a user standpoint
-What information needs to be sent from the algorithm to the visualization? Have a separate animation code that doesn't necessarily talk to the algorithm?
-Divide visualization into: animation, time control, user menu
-Different colors for key, plain text, encrypted highlight
-Make only one prototype so there's more to present to Prof. Joe Li (Target- 5/24)

- Takes in user input ★MH
- Provides proper encryption/decryption ★JF
- Can highlight table (hopefully text too) ★ YZ
- Some form of pacing (stepwise or controlled continuous) ★ MR

Yuyao: Worked on: Looked at other visualization tools, leaning toward pyGame as the final decision. Considered other ways to use different models. Found other sources, sent questions to others about how to use pyGame. Contacted creator of the other software for Vigenere cipher. Next: Communicate with contacts and creating a table in pyGame, learning how to do the animation. Holding back: learning pyGame.

Meghan: Worked on: Reading more about pyGame, how to use it and thinking about how to use specific functions for what we need. Considered memoization code for saving steps. Next: learn pyGame and how to translate encryption/decryption steps so pyGame can animate them. Holding back: time, working on other classes, learning pyGame.

Max: Worked on: looking into alternatives to flask server, created Github Repository. Programs that can compile the pygame files into an executable file we can send out. Found more citations for design specifications, with quotes. Next: Work on making a decision about which visualization tool to use. Holding back: learning pyGame.

Josh: Worked on: Researched best ways to implement encryption and decryption in python. Next: Get a working model of the encryption/decryption code. Holding back: time, working on other classes.

Meeting Notes for 5/14/21 at 3:00 - Meeting with Prof. Hornof

Additional Persons: Anthony Hornof
All in attendance
3:00 - 4:20

Topics to discuss

_√_ Organize meeting document
__ Review timeline plan
_v_ Discuss each individual member's progress
- What are your responsibilities on the project?
- What have you done in the last few days?
- What is your next task?
- What, if anything, is holding you up from accomplishing that task?

__ Discuss interactions with Professor Li
__ Discuss system building plan (What you'll build and how you'll build it)

Notes:

Yuyao: responsible for collecting information about how to do the visualization part. Just got started and found some helpful resources that we can use by using python, especially modules called matlib, pygame, dash, barchartrace. Next task: look more into it. Try to see if can plot table format based on libraries (evaluating libraries for ease of use/practical). Holding up: technical stuff: knowing how to plot table and how to do step by step animation. Suggestions: Meghan's book, save state for each step, pattern

Meghan: responsible for looking up visualization tools/techniques to show the vigenere cipher. Read through how pygame works (pygame book), best way to get interactivity from users (so far), meet with Yuyao next to discuss findings. May experience time constraints for the next task.

Max: responsible for findinding/reading research papers and getting the flask server set up with input fields. Has been working on SRS, SDS, got one paper quoted with a citation. Next, getting another citation or two then setting up a server with plain text and key input fields. Expressed being able to get a lot done over the weekend.

Josh: Responsible for researching articles to find more design specifications, needs to get started on cipher functionality (not visualization). Look into cryptanalysis if time permits. Hasn't had much time the last couple days, but has been able to look at a couple articles so far. Look into integrating cipher functionality with other modules nicely. Time constraints due to other classes.

Suggestions for leading meetings:

- Ask for specific answers
    - Be persistent
    - Rephrase questions
- Clarify Understandings
    - Did that help?
    - Did that answer your question?
- Lead the Discussion (with leading questions)

Action Items:
__ Joshua will find software pattern

Hard to make progress if tasks are too big. True for all projects. Specific tasks
please continue like this
figure out when to meet - “nice to meet in zoom with video” - “helps with group cohesion”
Come up with agenda items
when you look at the papers… looking for ideas for specific things to add to system/design based on what does/doesn't work.
Flask - do you need a flask server? Focusing on the visualization aspect. Go to the stakeholder: maybe he doesn't want a flask server?

Timeline and Assignment Spreadsheet:

	Task	Assigned To	Start	End	Dur	2021						
						4/25	5/2	5/9	5/16	5/23	5/30	6/6
	Vigenere Cipher Visualization Tool Project	JF / MH / MR / YZ	5/7/21	5/30/21	24							
1	Cipher: Basic Encryption	JF	5/7/21	5/14/21	8							
2	Cipher: Basic Decryption	JF	5/7/21	5/14/21	8							
3	Cipher: Testing Encryption/Decryption	JF	5/19/21	5/20/21	2							
4	Research: Visualization	JF / MH	5/11/21	5/13/21	3							
5	Research: Visualization Tools	MR / YZ	5/11/21	5/13/21	3							
6	Research: Existing relevant Software	JF / MH	5/11/21	5/13/21	3							
7	Menu & Buttons: Start Menu	MH	5/21/21	5/25/21	5							
8	Menu & Buttons: Main Input Menu	MH	5/21/21	5/25/21	5							
9	Menu & Buttons: Information	MR	5/26/21	5/29/21	4							
10	Menu & Buttons: User Input	MH	5/23/21	5/25/21	3							
11	Menu & Buttons: Animation	MR	5/22/21	5/24/21	3							
12	Game Functionality: Table Display	YZ / JF	5/22/21	5/25/21	4							
13	Game Functionality: Text Display	YZ / JF	5/24/21	5/27/21	4							
14	Game Functionality: Stepping	YZ / JF	5/24/21	5/26/21	3							
15	Game Functionality: Play/Pause	YZ / JF	5/24/21	5/26/21	3							
16	Game Functionality: Restart	YZ / JF	5/24/21	5/26/21	3							
17	Game Functionality: Speed control	YZ / JF	5/24/21	5/27/21	4							
18	**Milestone: Prototype**	Everyone	5/27/21	5/27/21	1							
19	Animation: Ciphers with table & Highlights	YZ / JF	5/25/21	5/27/21	3							
20	Animation: Text Highlights with table highlights	YZ / JF	5/25/21	5/28/21	4							
21	Animation: Control button functionality	YZ / JF	5/26/21	5/28/21	3							
22	Integration: Integrate main input menu and visualization scene	MH / JF	5/25/21	5/28/21	4							
23	Integration: Integrate main input menu and cipher functionality	MH / JF	5/25/21	5/27/21	3							
24	Integration: Integrate Table and Pacing modules	JF / YZ	5/25/21	5/28/21	4							
25	Integration: Integrate all Info & Menu scenes	MH / MR	5/26/21	5/27/21	2							
26	Integration: confirm navigable	MH	5/27/21	5/29/21	3							
27	Testing	Everyone	5/29/21	5/30/21	2							

Project 2 Timeline

Group: **Group 3**

Team Members (and initials): **Joshua Fawcett (JF), Max Hopkins (MH), Meghan Riehl (MR), Yuyao Zhuge (YZ)**

Date this was last updated: **5/31/21**

Last updated by (whom): **Everyone**

key:

Begin By	Started
Due	Slack Time
Done-MR	Overdue
Special	

* If a task is started on the begin by date, change only the cell color to:
* If a task was completed on the due date, change only the cell color to:
* A task completed within slack time is not considered overdue
* A special cell is something not covered by the other options, delays, changes, etc. Please provide more information in the cell.
* When a task is completed another team member will initial the cell confirming completion

Grouping	Task or Milestone	Assigned to	5/5	5/6	5/7	5/8	5/9	5/10	5/11	5/12	5/13	5/14	5/15	5/16	5/17	5/18	5/19	5/20	5/21	5/22	5/23	5/24	5/25	5/26	5/27	5/28	5/29	5/30	5/31
Project Planning					1hr x 4			50min x 4	55min x 3	2.5hr x 4		1.5hr x 4				35min x 4			20min x 3				1:15 x 4	1:10 x 4		50min x 4		
	Group Meetings	Everyone			3:00 PM			1:30	12:00 PM	4:30		3:00 PM				12:00 PM			3:00 PM				12:00 PM	3:50 PM		3:00 PM			12:00 PM
	SRS	Everyone				Begin By		Started		Initial	Revisions														Final				
	SDS	Everyone				Begin By			Started	Initial	Revisions														Final				
	Project Plan	Everyone				Begin By			Started	Initial	Revisions														Final				
	Programer Documentation	Meghan/ Josh									Begin By														Due				
	User Documentation	Yuyao/ Meghan									Begin By														Due				
	Read Me	Josh/ Max									Begin By														Due				
	Installation Guide	Max/ Meghan									Begin By														Due				
	Presentation Power Point	Everyone																							Begin By				Due
Cipher Functions																													
	Basic Encryption	Josh												Due		Done (1hr													
	Basic Decryption	Josh												Due		Done (1hr													
	Testing Encryption/Decryption	Josh														Due	Started	Done-MH											
Research																													
	Visualization	Josh/ Max															Due												
	Read/ Summarize Papers	Josh/ Max							Started		Done-MR						Due												
	Citations	Josh/ Max							Started		Done-MR						Due												
	Visualization Tools	Meghan/ Yuyao																											
	PyGame/Dash	Meghan/ Yuyao														Done-JH													
	Integration with user interface	Meghan/ Yuyao														Done-MH													
	Download package/ website application	Meghan/ Yuyao														Done-MH													
	Existing Software research	Josh/ Max							Started		Done-MR						Due												
Game functions																													
	Menus/ buttons																												
	Start Menu	Max																								Done-JH			
	Main Input Menu	Max																	Started				Done-YZ						
	Information	Meghan																						Started			Done-JH	Due	
	User Input	Max																			Started		Done-JH						
	Animation	Meghan																	Done-JH										
	Animation																												
	Table	Yuyao/ Josh																		Started			Done-MH						
	Stepping functionality	Yuyao/ Josh																				Started			Due-MH				
	Play/pause functionality	Yuyao/ Josh																				Started		Done-MR					
	Restart functionality	Yuyao/ Josh																				Started		Done-MR					
	Speed control	Yuyao/ Josh																				Started		Done-MR					
Prototype		Everyone																				Due		Done-MR					
Integration																													
	Integration																												
	Integrate main input menu and visualization scene	Max/Josh																	Started				Done-YZ						
	Integrate main input menu and cipher functionality	Max/Josh																	Started				Done-YZ						
	Integrate Table and Pacing modules	Josh/Yuyao																						Started		Done-MH			
	Integrate All Info/Menu Scenes	Max/Meghan																					Started			Done-JH			
	Confirm navigable	Max																	Due							Done-JH			
	Animation																												
	Ciphers with table/ hightlights	Yuyao/Josh																				Due	Started		Done-MH				
	Text Hightlights with table hightlights	Yuyao/Josh																				Due	Started			Done-MH			
	Control button functionality	Yuyao/Josh																				Due		Started	Done-MR				