Coursework Report

Lee Robinson - 40288694
40288694@live.napier.ac.uk
Edinburgh Napier University - Module Title (SET08101)

1 Introduction

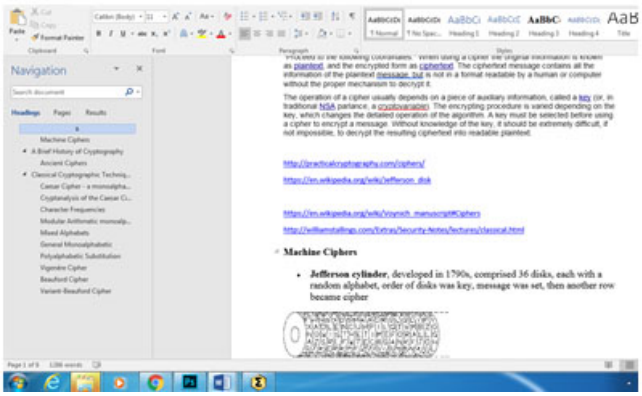
This assignment aims to demonstrate competent use of HTML, CSS and JavaScript, by implementing a website about classical ciphers. It is a pretty small site with the main emphasis on clarity, aesthetics and functionality. I decided to implement 3 ciphers, Caesar, Hill and Vigenère.

Caesar was the most simple and used to get to grips with JavaScript, and Hill was chosen to really test myself and to demonstrate a fairly complex example with good functionality - it makes use of the properties of invertible matrices which makes it far harder to crack but also far more challenging to code. Vigenère sits somewhere between the two.

Most of my reading was done on wikipedia.org, williamstallings.com, and khanacadamy.org to get to recap on Matrices and how to find Inverse Matrices. I also used w3cschools.com for any HTML, CSS or JavaScript related information.

2 Design and Implementation

It was difficult to totally separate the design and implementation process sections. Being the first full site I have made from the ground up, and also being relatively small, the two tasks were intertwined from start to finish, and so I have merged the two for the purposes of this report. The design process started out as simply reading about the subject of classical ciphers, and deciding on content. I then collated the links to the sites I was studying and various images I could possibly use into a word document.

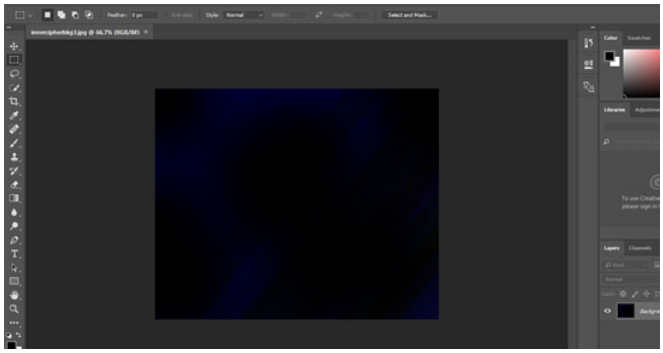


Screenshot-1. - Collated Information Document

Then I typed out the base content for index.html

Screenshot-2. - Rough Content Design Document

The layout was kept simple, and required creating just a header, and then several variations of a main background. In the end I decided to actually scrap a separate heading image altogether.



Screenshot-4. - Background Design

The original site layout was as follows:

Original Site plan:

index.html - introduce site and also talk about what ciphers are.

design.html - information regarding site styles.

cipher1.html - separate page with useable ciphers coded in JavaScript. Will also talk about the cipher and how it works.

cipher2.html - as above.

cipher3.html - as above.

style.css - style definitions.

scripts.js - site scripts

The ciphers will each be implemented on a single page and the descriptions on a linked popup page, or vice versa.

Implemented Site Plan:

index.html - introduce site and also talk about what ciphers are

design.html - information regarding site styles.

classical_ciphers.html - separate page with ciphers coded into JavaScript, each cipher has it‘s own clearly defined section akin to a separate page, just all on one page for ease of navigation.

Descriptions of ciphers were implemented using popup overlays. The decision to have the ciphers on one page, but in clearly separated sections was to try guide the user through the site, first reading down the page through the introduction of classical ciphers and cryptography, and then navigating to (maybe) the first cipher at the top of the classical_ciphers.html page. I felt this made the site more of a rewarding user experience.

3 Critical Evaluation

I believe the site offers a fairly rewarding experience in terms of aesthetics, ease of use, and functionality. I felt 3 ciphers would be sufficient for the purposes of this evaluation, one of the main reasons being that it was fairly challenging to implement the Hill cipher without the use of additional libraries (such as JQuery), and it required substantial background reading and revision on Matrices.

The Caesar cipher was chosen as an easy choice to learn the ropes of JavaScript, and once I was comfortable, I felt that the Vigenere was a step up that would be easy to code after completing Caesar, as a slightly advanced variation.

The decision to implement the Hill cipher was very challenging but hugely rewarding as it seems to work well, without the user having to know anything about matrices. If the the user is slightly more knowledgeable and wishes to try several matrices they know to be invertible (or not), then the system should encipher the text, or advise the user that the given matrix is not suitable.

All of the cipher descriptions are given in popup boxes, which darken the rest of the pager, so to focus the users attention on that which they have navigated to, again the aim is to guide the user for a more rewarding experience.

I believe I could have gone into more detail with regards to how the cipers worked, especially the Hill and Vigenère cipher but time constraints (compounded by the time taken to implement the Hill Cipher) made it difficult. I could have also added more ciphers but again, time constraints made this difficult.

Overall I believe this to be a good implementation when compared to the requirements initially set out. I believe it is easy to navigate, clear, fairly pleasing on the eye, and functionally sound. I also believe I have gone beyond the core teachings to deliver a fairly complex cipher in the Hill Cipher, which meant coding matrix inversions and related functions with only the core JavaScript library. I doubt the code is in it‘s simplest and most elegant form, but this is something I anticipate improving with experience. I would also like to customize the site further allowing for alternative displays for different devices - the layout of classical_ciphers.html definitely is not optimized for a great mobile experience.

4 Personal Evaluation

On a personal level I am extremely pleased with my work. Initially getting my head round positioning div‘s seemed like a terrifying nightmare, but that quickly started to make sense. JavaScript is an enjoyable language to use due to it‘s relaxed attitude with regards to assigning variables compared to other languages. My choice of ciphers (namely "Hill"), whilst challenging, upon achieving a working script, gave me huge personal satisfaction. There ware several moments when I thought I may have to abandon the choice of ciphers in favor of something where I perhaps had a better grasp of the Maths involved, but persistence paid off. I have Khan Academy to thank for that.

I feel as though I now have a good grasp of HTML, CSS, and JavaScript. I also learned how design and implementation can be intertwined, and so you must remain flexible with your approach. I know of course there is much room for improvement, from a user experience perspective; perhaps better use of space and/or graphics, and improved layout. I also feel that with more experience, I can improve my performance in the design phase with the result that I can perhaps finish the project sooner, and/or include more content/functionality.

Overall I enjoyed the project, felt I learned a substantial amount, and also felt as though I produced a solid piece of work. The experience so far will definitely serve as a strong foundation moving forward.

References

[1] Image of Jefferson Disc. Digital Image. *Introduction to Cryptography.*. n.p. 22 Feb 1996. Web 3 Feb 2017
http://williamstallings.com/Extras/Security-Notes/lectures/figs/classical4.gif

[2] Image of Wheatstone Disc. Digital Image. *Introduction to Cryptography.*. n.p. 22 Feb 1996. Web 3 Feb 2017
http://williamstallings.com/Extras/Security-Notes/lectures/figs/classical5.gif

[3] Image of Enigma Machine. Digital Image. *Introduction to Cryptography.*. n.p. 22 Feb 1996. Web 3 Feb 2017
http://williamstallings.com/Extras/Security-Notes/lectures/figs/classical7.gif

[4] Dr Laurie Brown. *Introduction to Cryptography.*. n.p 22 Feb 1996. Web. 3 Feb 2017
http://williamstallings.com/Extras/Security-Notes/lectures/classical.html

[5] Photo of Dr Lester Hill. *Lester Hills "The checking of the accuracy" - finally completed* .
https://wdjoyner.files.wordpress.com/2015/03/hill_lester_s.jpg

[6] Portrait of Blaise de Vigenère. *Portrait by Thomas de Leu.*. From English Wikipedia.
https://en.wikipedia.org/wiki/Vigenere_cipher#/media/File:Vigenere.jpg

[7] Scultpure of Julius Caesar. From historyonthenet.com
https://www.historyonthenet.com/julius-caesar/