Marc McIntosh Web Technologies coursework

40317980

March 8, 2019

1 Introduction

I have been tasked with creating a website from scratch that can be used to encode and decode plain text messages with a variety of different ciphers. The site will be written in HTML and CSS with JavaScript being used to process the plain text messages into cipher text and vise-versa.

The site will be designed to be operated by an inexperienced user with minimal to no instruction as so must have a sleek and intuitive design allowing for easy operation. This will include making the site as minimalistic as possible without impeding functionality, for example this could include only operating the site on a single page in order to reduce the navigation required by the user to peform a specific task. The site should also capable of handling multiple types of ciphering techniques such as Cesar Cipher, Vigenere Cipher, ROT13 and morse code.

2 Software design

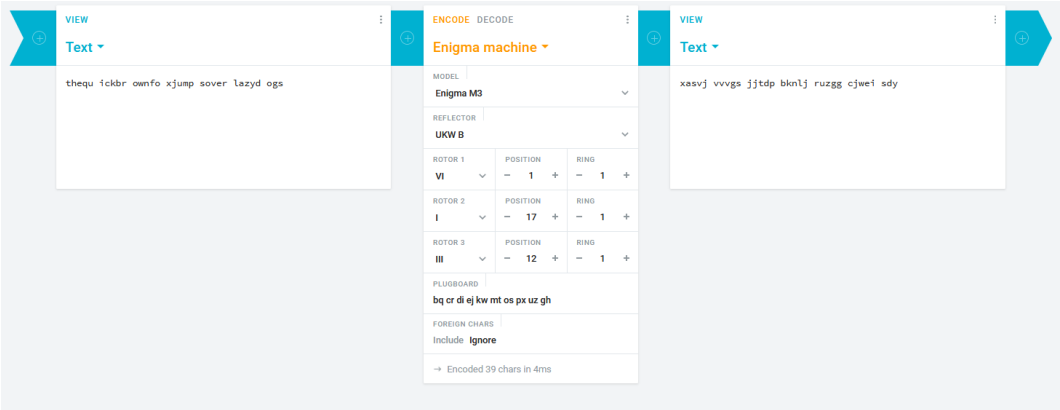
I have derived a list of requirements that I think are necessary in order to create a pleasant user experience while also making it easy to update and maintain. These requirements are as follows.
• The site must be easy enough to use that a user can still have full control after only reading minimal or no instructions on how to function the site
• The site must be designed that newer ciphers can be added easily without much modification • Must have the capability to encode in the Caesar cipher, Vigenere cipher, ROT13 and Morse code

In order to gain inspiration as well as an understanding of what design could make for a good Cipher web page I decided to look at other popular sites. Figure 1 shows a screenshot of the website https://www.dcode.fr/.

After using dcode.fr as a cipher tool I have concluded that it has a number of factors that I think would be beneficial to add to my own site. The first point is that the site provides detailed information about each cipher selected allowing the user to easily become more informed about the cipher they are using. However the sites layout makes it seem outdated and combined with large paragraphs of text could make it seem daunting to users who have never been exposed to cryptography before, also a more updated user interface may make it look more graphically pleasing increasing the quality of the overall user experience. This will be taken into account when I am designing my own site.

Figure 1: Main page of dcode.fr

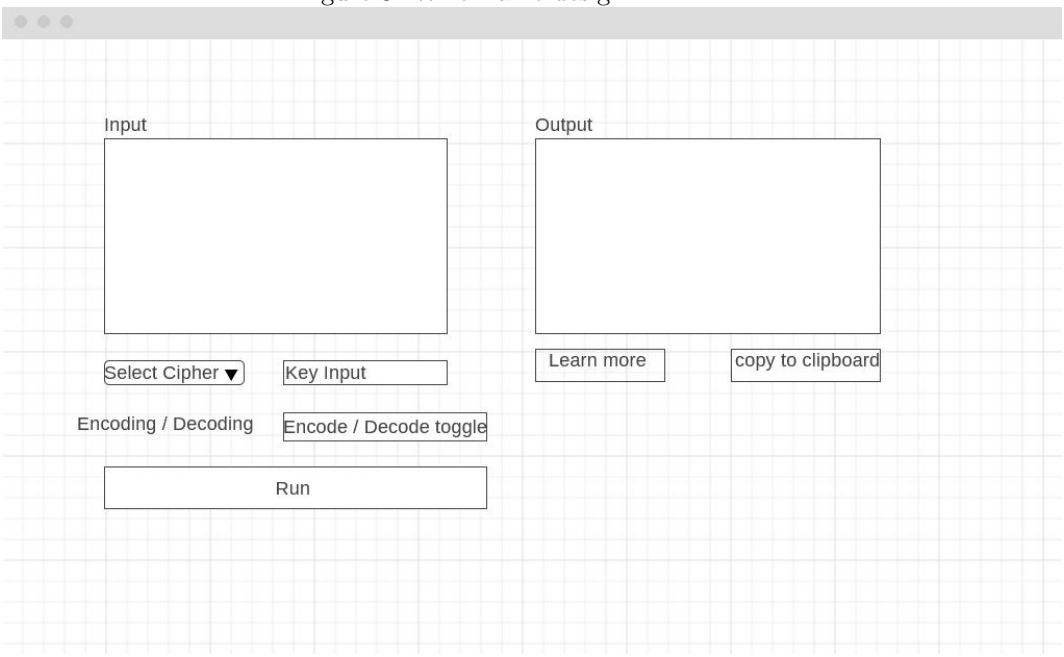
Figure 2: Main page of Cryptii



The next site that I looked at was Cryptii.com which has a far more up to date and modern looking user interface as well as having a more modular design compared to dcode.fr. However unlike dcode.fr, cryptii does not provide any information regarding how the cipher works which I think may be a down fall. This will be taken into consideration when designing my own site. Also Cryptii.com has many options on how to each cipher, which may be beneficial for experience users however could also be confusing for inexperienced users.

Using the research I gathered I started the design of the site using an online wire-framing tool to quickly generate a layout of what I want the site to look like. This has the benefit of allowing me to see what the site will look like without having to send much time converting each design to code as this would be an inefficient use of time. I wanted to design a site that was easy to use to inexperienced users and so had to create a user interface that was minimalist without losing functionality

Figure 3: Wire-frame design

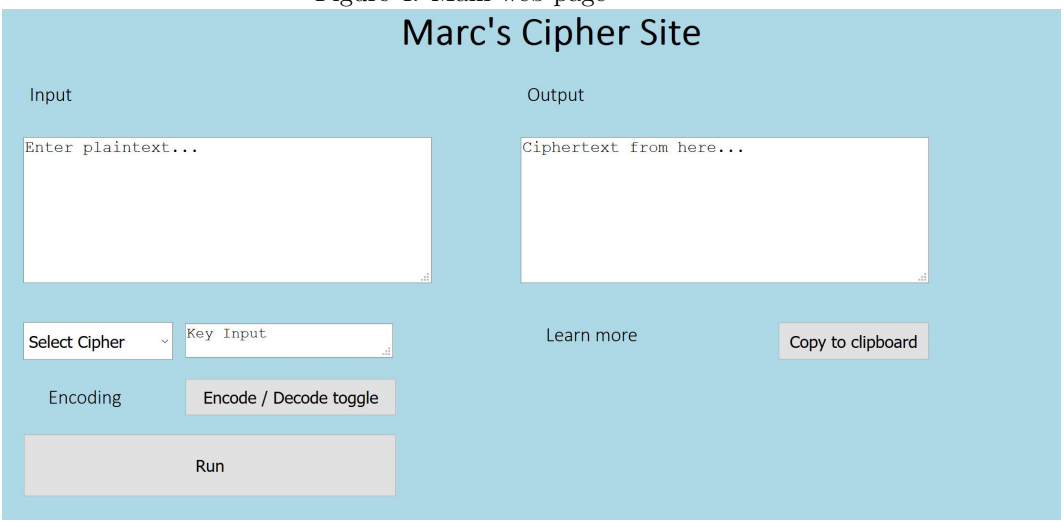


The cipher is first selected using a drop-down box to where the can chose from multiple options. Due to each cipher either requiring a specific type of key or no key at all I will implement a system that explains to the user what format the key should be in for the cipher to work. I will also implement alerts to inform the user when mistakes in the input have been made.
In order to make the site as simple as possible encode and decode functionality use the same page, however are toggled between Encode and Decode using the "Encode / Decode toggle" button.
Once the user has configured the input message, cipher and key, they then need to press the "Run" button. I have also added a "learn more" feature that redirects the user to the Wikipedia article of the cipher that have currently selected. I have also added a "Copy to clipboard" button as the user usually requires the output for something else they are doing and so need to copy the result.

3 Implementation

After the design was complete I started with creating the basic layout in HTML and CSS giving me a basic shell to work with when implementing the JavaScript.

Figure 4: Main web-page



After this was achieved I started to think about how I would design the layout of the JavaScript code. As specified I wanted to make it easier for other developers to add new features and ciphers so I made the main function compare the name of the cipher and if it returns true then that ciphers specific function would run. This means that all the developer would have to do to add a new cipher is add the new name of the cipher to the drop-down box in the HTML as well as creates it own function, which has the affect of reducing development time.

4 Critical evaluation

After completing the site I began testing it against the evaluations I stated in the software development stage. To find a user that could test the functionality of the site I asked my father as he had no experience with using Ciphers or Cipher websites before. To conduct the test I asked him to perform instructions like "encode your name with the Caesar cipher" with no other guidance on how to use the site. After only a brief stage of confusion my father was able to complete the task without needing outside help. This has made me conclude that I have fulfilled this requirement.

The second requirement was that it would be easy for other developers to implement more functionality due to well designed code, however I was not able to find anybody with JavaScript knowledge to test this against, resulting in having to timing myself how long it took me to implement and debug a new cipher from scratch. The cipher I decided to create was the "ASCII shift" cipher which is similar to the Caesar cipher however uses the whole ASCII range and so can have a key between 1 - 128. This took me 22 minutes to implement which as I have nothing to compare it to, is less useful, however I feel that if I has not designed the JavaScript layout the way I did, it would have taken far longer and so I am also considering this requirement fulfilled.

The third requirement was to include the ciphers Cesar, Vigenere, ROT13 and Morse code. This has been implemented and are working correctly and so I conclude that I have fulfilled this requirement.

5 Personal evaluation

One way that this site could be improved is through adding more ciphers. This would have made it more enticing for users to visit and so would have resulted in more traffic.

A cipher cracking function could also have been implemented which would have allowed the user to possible crack a cipher without knowing the original key. This would have been especially useful for user who play in CTF (Capture the flag) competitions as this can sometimes involve cracking codes. This would have further increased the popularity of the site.