

Coursework Report

Cool Student
4008000@napier.ac.uk
Edinburgh Napier University - Module Title (SET00000)

1 Introduction

1.1 Goal

My goal for this coursework assignment was to implement a website dedicated to enciphering messages using different ciphers. The site needed to have at least two different ciphers that encrypted input from the web user. It also required JavaScript files for each cipher as well as a design.html page that was focused on listing all the different styles and topographical elements of the site in one place.

1.2 Overview

I had decided to implement three different ciphers for my site with the option to both encrypt or decrypt input the web user gives. I wanted to go for a minimalist theme with a straight-forward user-experience. The first cipher is the Caesar Cipher which shifts the index of the letters in the alphabet by an "x" amount. The second is the Atbash Cipher which is dedicated to reversing the letters of the alphabet. And lastly, I had originally planned to fully implement the Substitution Cipher which would allow for multiple ways of encryption with a customizeable key but ended up only being able to implement a portion of it, being the Alphabetical Substitution Cipher. This was caused due to more time being spent on error-proofing than expected. However, it did not get in the way of developing a cohesive enciphering site that has commendable functionality with the features it provides.

2 Software Design

2.1 Sketches

The first step I took in my software design planning was sketching any ideas I had for the site. Before starting any sort of research, I wanted to gather my thoughts on how I would visually piece together the looks of the site by sketching them out. When sketching I tried to take into account different formats on how the site could look like in order to analyze what would be the easiest to navigate (Figures 1-3). This greatly helped me in my later research since it allowed me to find out which of the formats were the most efficient to both implement and use. What would end up happening is that I would use portions of each sketch as inspiration to put together what I thought would be the most straightforward design for the user-experience.

2.2 Cipher Selection

Before starting at the Caesar Cipher as mentioned in the assignment sheet, I wanted to look for other ciphers on my own

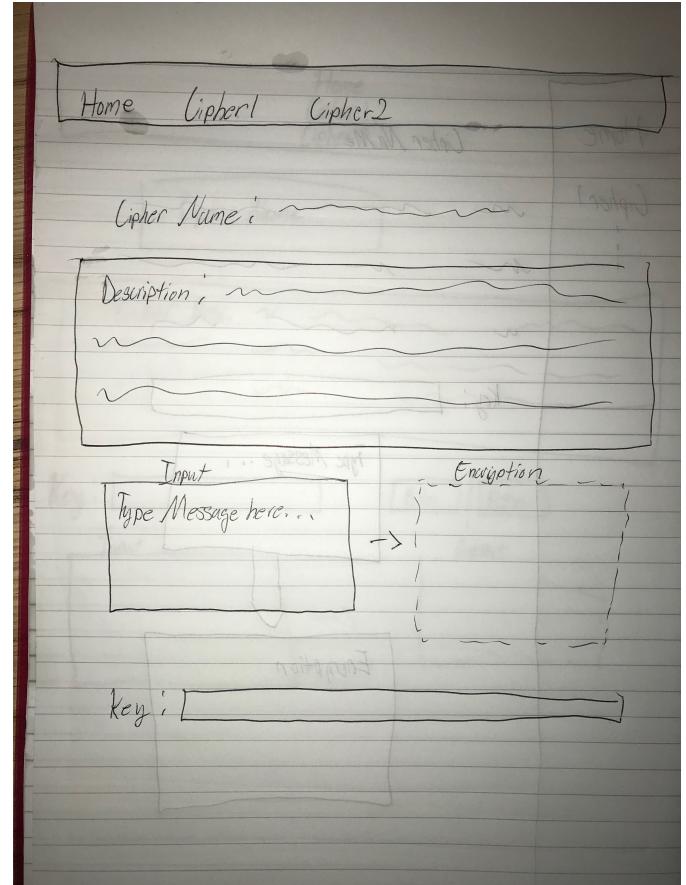


Figure 1: Sketch 1

in order to avoid any influence on what I needed to implement. I first started on a website called Rumkin which had a section that listed many different kinds of ciphers [1].

Atbash Cipher I decided to choose Atbash first since I had heard about it and was interested in its developments. I found that it would give me a good base start in developing my logic for how to go about enciphering and deciphering before I moved on to the more difficult ciphers. Upon reading more into Atbash, I found that it is considered a substitution cipher [2].

Caesar Cipher This led me into finding out about other substitution ciphers. Of course the most popular being the Caesar Cipher [3]. I chose to implement this cipher at that point since it seemed that it built logically more off of something like Atbash but with a key involved.

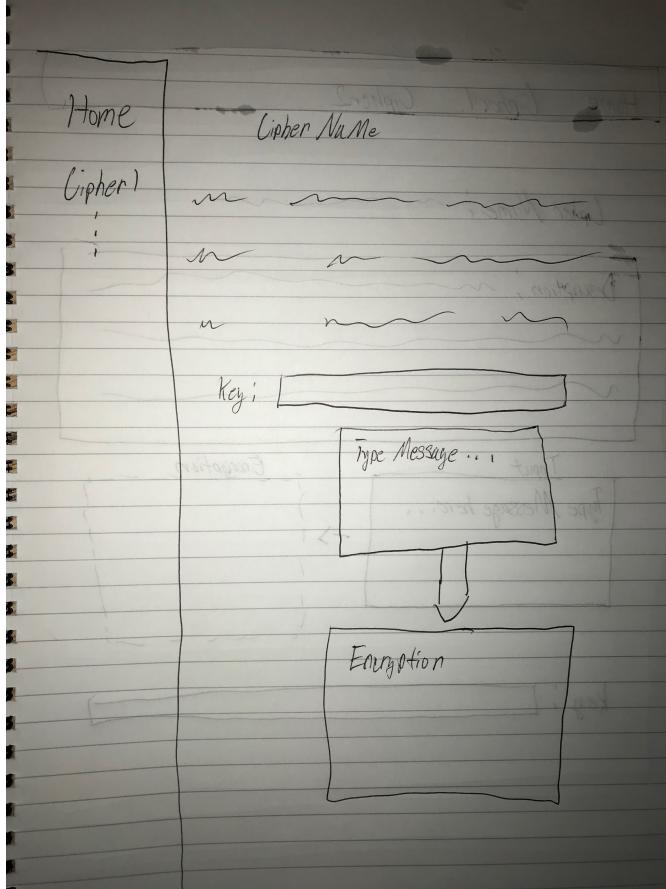


Figure 2: Sketch 2

Simple Substitution Now that I had chosen two ciphers where one built off of the other, I decided to look for something a step above the Caesar Cipher to implement. Through further research, I had found that the Substitution Cipher in general could be implemented. This seemed more of a challenge since it gave more freedom to the user but also seemed measurable since the logic could be built further from the Caesar Cipher. I got the inspiration based on another cipher site that implemented just that [3].

2.3 Design

The next thing I did was try and look for any designs online that somewhat matched the ideas from my sketches to try and use as inspiration. I first tried taking a look at different language translation websites since I thought that those would be the next closest type of site to the one I was focusing on developing.

Color After looking at Google Translate, Reverso.net, Translate.com, and others, I noticed that the colors were usually bright but soft on the eyes. For example, on Translate.com and Reverse.net, there was a strong sense of blue and that the other colors would not wash out the blue. This influenced me into wanting to make my site around blue since most translation sites had that as a theme.

Blueprint After deciding on the what color the theme would be, I decided to look at design templates around blue for inspiration. I also decided to take a look at site designers

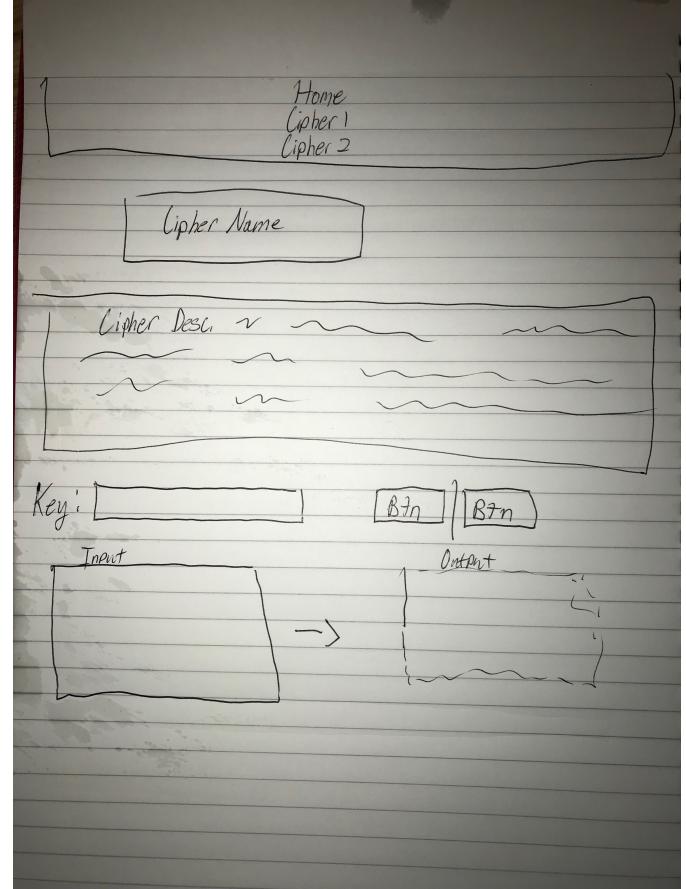


Figure 3: Sketch 3

rather than site designs in order to find more consistent pieces of work to grab ideas from. One site in particular that helped with that was Dribbble.com which brought me to a designer that posted an animation outlining a translate page [4]. This is what became the main inspiration for the design of my site.

3 Implementation

3.1 Navigation Bar

The navigation bar was implemented using a W3 tutorial for turning a list of links into a bar using CSS (Figure 4). It has set colors for its default state, when it is hovered over, and for the active page.



Figure 4: Navigation Bar

3.2 Home Page

The home page simply displays a welcome message that directs users to use the navigation bar in order to redirect themselves to the different ciphers' pages (Figure 5).

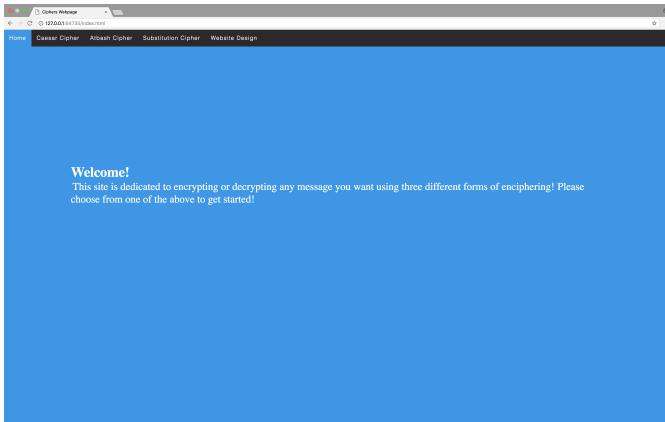


Figure 5: **Home Page**

3.3 Caesar Cipher Page

The Caesar Cipher page is implemented using divs for the containers of the various elements in order to have them styled nicely (Figure 6). At the top of the page is the title of the cipher as well as the description. The page includes a textarea for the user's input and another readonly textarea for the output. There is a number-only input for the shift/offset in the cipher and two buttons for both encrypting or decrypting the input. The encryption/decryption works by mapping out a new alphabet that is dependent on the shift. That is then used in comparison to the original alphabet in order to get the indexes of the input for the output. The encryption/decryption also ignores any special characters and/or numbers as well as any empty space.

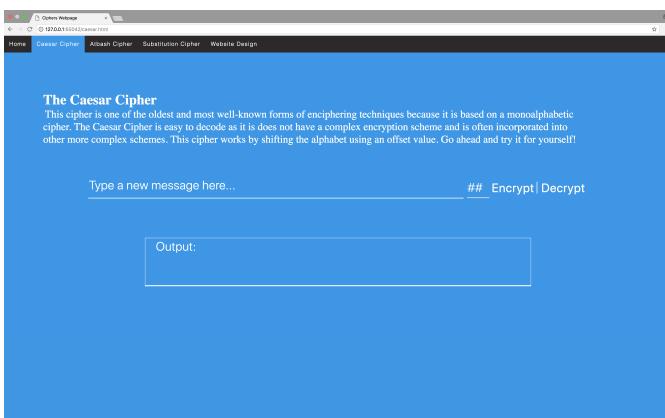


Figure 6: **Caesar Cipher Page**

3.4 Atbash Cipher Page

The Atbash Cipher Page works in almost the exact same way as the Caesar Cipher Page except for the fact that it uses no shift/offset input. (Figure 7).

3.5 Substitution Cipher Page

The Substitution Cipher Page includes all the same elements of the Caesar Cipher Page and more. It additionally has an another textarea for the user to generate their own key, and a span above it that shows what letters of the alphabet are yet to be used. If the user types in duplicate letters, spaces, or

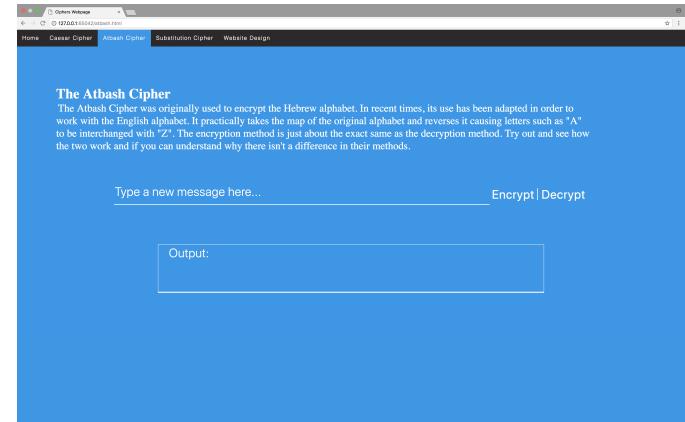


Figure 7: **Atbash Cipher Page**

special characters, then the user will be alerted and prompted to fix the issue. The span also will say what letter is used more than once as soon as the user has been alerted of the issue (Figure 8).

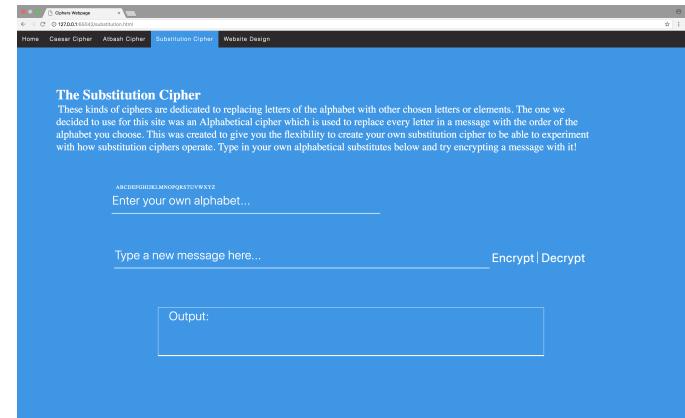


Figure 8: **Substitution Cipher Page**

3.6 Website Design Page

This is the design.html page which displays all the different graphical and styled elements that are used in the site (Figure 9).

4 Implementation Evaluation

4.1 Requirements

When it comes to the requirements that were set out, the site reaches all of them. The site includes more than two ciphers, has an index.html that is used as the home page for users to navigate from, and a design.html page which lists all the different presentational elements of the site. The site is also fully implemented using only HTML, CSS, and Javascript without using any extra libraries, frameworks, or templates.

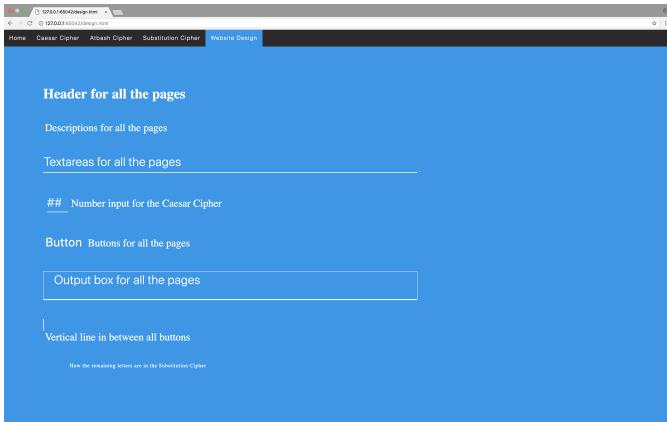


Figure 9: **Website Design Page**

4.2 Improvements

An improvement that could have been made, for example, was giving the user the ability to use special characters as part of their key for the Substitution Cipher. Another one could have been adding the function of clearing the invalid entry for the user in the Substitution Cipher page rather than just alerting them. Additionally, there could have been more options of adding additional keys or key mutators to the Substitution Cipher, such as, encoding the output as a set of particularly chosen images rather than only encoding them as text [5]. There could have been more responsiveness to the site's styling so that re-sizing of the page wouldn't affect the design in any negative way. Lastly, the textareas that don't allow certain characters should have been stopped from being typed in all together.

5 Personal Evaluation

5.1 Reflection

Looking back at the development for the site, I wish I had found more interesting ciphers other than ones that were already well-known. Though, I had found greater motivation when thinking about how I was going to style the site with the small amount of elements that each page would have. In the past, I've always seen a lot of empty space on a page as difficult to fill in. I usually would feel like I didn't know what to do with all the space unless I had enough elements to take its place. I had gotten this assumption when looking at other sites with minimal amount of items on a screen.

5.2 Execution

But this time, I decided to take the opportunity of this project to really delve into designs that sport more of a minimalist look. It really opened my eyes to see how a page can be structured with very little on the page. In the past, for example, I would have probably used multiple drop-down option menus for each letter in generating keys in order to use up more space that is available on the page. However, the research for designing a project such as this was surprisingly more fascinating since I was trying to make the page have less but do more.

5.3 Conclusion

In conclusion, I feel like I performed as well as I was able to with the resources that I had. Finding motivation in my design vision as well as in my design fascination helped push me through all the time spent doing mundane acts such as error-proofing or debugging code. It allowed me to have a good balance between juggling the site's services with its looks which is why I believe I was able to deliver a well-rounded and respectable site.

References

- [1] "Cipher tools." <http://rumkin.com/tools/cipher/>. [Online; accessed 25-May-2018].
- [2] "Atbash." <https://en.wikipedia.org/wiki/Atbash>. [Online; accessed 25-May-2018].
- [3] "Substitution cipher." <https://www.britannica.com/topic/substitution-cipher>. [Online; accessed 25-May-2018].
- [4] E. Julliot, "Translate." <http://practicalcryptography.com/ciphers/simple-substitution-cipher/>, August 2015. [Online; accessed 25-May-2018].
- [5] "Substitution cipher." <http://rumkin.com/tools/cipher/substitution.php>. [Online; accessed 25-May-2018].
- [6] "Coolors." <https://coolors.co/>. [Online; accessed 25-May-2018].
- [7] "How to check if character is a letter in javascript?." <https://stackoverflow.com/questions/9862761/how-to-check-if-character-is-a-letter-in-javascript>. [Online; accessed 25-May-2018].
- [8] "Validate textarea to accept only characters no special symbols or numbers." <https://www.codingforums.com/php/288101-validate-textarea-accept-only-characters-no-special-symbols-or-numbers.html>. [Online; accessed 25-May-2018].
- [9] "Css navigation bar." https://www.w3schools.com/css/css_navbar.asp. [Online; accessed 25-May-2018].