

Coursework Report

Darwon Rashid
40280334@napier.ac.uk
Edinburgh Napier University - Web Technologies (SET08101)

1 Introduction

1.1 Brief History

People have been transferring messages between each other ever since humans have figured out how to write on stone. The difference between the early cavemen and the humans of today is that people now can transfer messages effortlessly across continents in less than a second. Humans have been improving means of communication for each century they have been on this planet. Nowadays people communicate with one another across the globe by using devices such as computers or smart phones without any concern of privacy. However, throughout history, there were many instances in which wars were won just based on the fact that one side intercepted the other side's means of communication. People later on started to encrypt their messages to protect the contents of their messages, so there were many forms of techniques called ciphers that were invented to encrypt messages.

1.2 Aim

This assignment involves the incorporation of certain ciphers in a website that was made by using certain web technologies. The aim of this assignment is to allow users to use a variety of techniques to encrypt and decrypt their messages while using a website with an interface that is user friendly and presentable. The ciphers chosen are different in technique and structure to inform the user of the many different ways of encrypting and decrypting messages. The ciphers are also taken from vast different periods of time to showcase to the user the advancement of ciphers over time. The website contains general information on ciphers and more detailed explanation of each cipher mentioned above.

1.3 Ciphers

The ciphers chosen for this assignment include the Caesar Cipher, Playfair cipher, Rail Fence Cipher, and Simon Wells Cipher. More details about each of the following ciphers are included in the web page of each specific cipher.

1.3.1 Caesar Cipher

Invented by Julius Caesar, the Caesar Cipher is one the simplest ciphers for users to grasp who do not know much about ciphers. It is a good starting point into ciphers, and it is interesting to see how ciphers were used in ancient times.

1.3.2 Playfair Cipher

Invented by Charles Wheatstone, the Playfair cipher is for users who want something more advanced. This was chosen

to showcase the complexity of ciphers, and how matrices can play a role in ciphers.

1.3.3 Rail Fence Cipher

This cipher is more visual than the rest of the ciphers. A rather straightforward cipher that depends on transposition. This showcases how certain ciphers can be graphical.

1.3.4 Simon Wells Cipher

This cipher is a combination of the Playfair and Caesar Cipher, and is here to show the user how anyone can construct a cipher and start encrypting messages.

1.4 Background Reading

Background reading for the information on ciphers came from the websites called Wikipedia and Braingle, while background reading for certain aspects of implementation came from the websites called Stackskills, Google's Material Design Documents, and W3Schools.

2 Software Design

2.1 Initial Plan

Initial design of the website first started on paper to figure out before any code how it should look and function to the user. The decision was to go towards a design that is inspired from Google's Material Design. The idea was to have cards that are positioned in a grid-like manner spaced out in the web page to group relevant information so it is easier for the user to read through information and navigate through the web page.

The website was to have a home page where it gives a brief overview of ciphers and the some other relevant information. Each cipher would have its own page with detailed information on the specific cipher and functionality to encrypt and decrypt messages. Navigation between pages initially was just a tab below the header for the page as shown below.

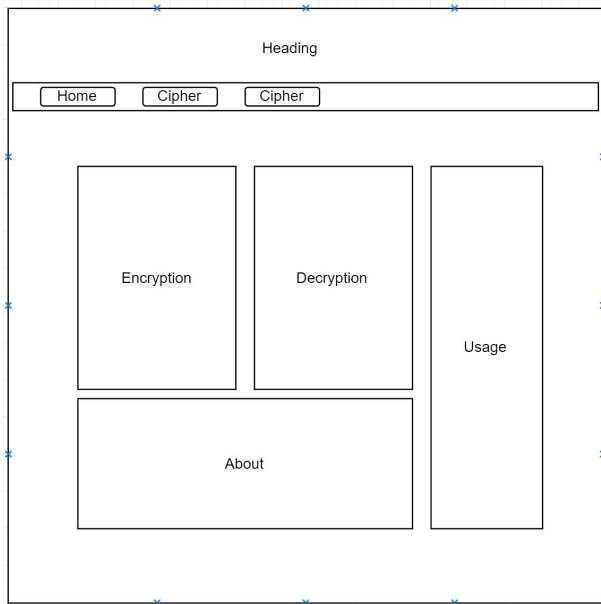


Figure 1: Desktop Mockup Design

2.2 Design

After seeing the way Google Translate handles input and output, it was best to have encryption in one card and decryption in another card both right next to each other, while having a side card explain how to encrypt and decrypt.

Colors for the website was picked while using Google's own Material Design Color picker. It is a tool that takes a chosen color and shows a set of different colors that compliment the chosen color to be used in any sort of User Interface.

Later on, navigation between web pages was later designed as a side navigational bar that slides from the left side when the user clicks on the button to view it. When it appears, the user then can navigate through the pages by clicking the name of the cipher the user wants to visit. Making the side navigational bar appear only when the user wants to view it makes it one less distraction from what the user is viewing at that current page. By positioning the button to stay always on the left side of the header with the shape of it being of the hamburger icon, it creates a clear consistent design throughout all the cipher pages. By having the layout of each cipher page be almost the same with the exception of how input for keys are handled, it creates familiarity so that when the user has figured out how to use one of the pages, the user will be able to navigate through the rest without learning how to navigate again.

A huge part of how cards look and feel depend on the shadows around it. It is a vital design aspect is an important aspect of Google's own Material Design. It gives the cards a sense of physical space that the user can see and interact with. The side navigational bar also has box shadow so it looks like it is overlapping what is on the screen. This aspect carries over to even inputs like the text area and buttons to stay consistent all around with the design.

2.3 Mobile Design

Having the layout of the website as cards allowed for a responsive design that wasn't hard to achieve due to the nature of grids. Since information was laid out in cards, to make the

website mobile friendly, all that needed to be done was to have the cards come after one another for there isn't much width on mobile phones to view three cards side by side. Navigating between the pages is still possible because the side navigational bar is accessed by pressing a button which is small enough to fit on mobile. All that's done to change the side navigational bar was to make the text of the links a little smaller. Having the cards change position depending on the size of screen adds on the notion of cards having a sense of physical space. This design is shown below.

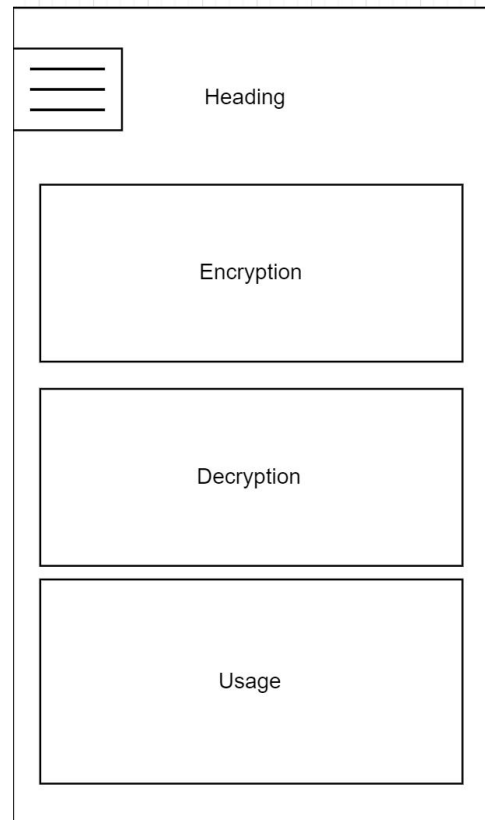


Figure 2: Mobile Mockup Design

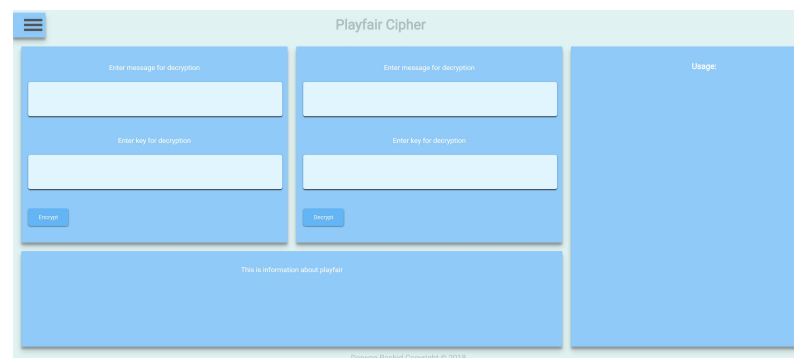


Figure 3: Final Desktop Design

3 Implementation

3.1 Organization

Once the design of the website was planned out, the implementation was next. Since this involved the usage of HTML, CSS, and JavaScript, the first step was to organize the files

in a manner that is easy for anyone to understand when viewing the source code. Each cipher page had its own HTML document along with a JavaScript file that included the functionality for encryption and decryption. There is one CSS file that acts as the only style sheet for the website. There is also an utility JavaScript file that includes helper functions that are used throughout each cipher's JavaScript file. For example, each cipher outputs its encryption/decryption to the other side, instead of having repeated code littered through out the files, it is condensed to two functions that are called from the utility file. The two functions are shown below.

```

1 function outputEncryption(cipher, key)
2 {
3   document.getElementById('encryptKey').value = key;
4   document.getElementById('decryptKey').value = key;
5   document.getElementById('decryptInput').value = cipher;
6   document.getElementById('encryptInput').value = cipher;
7 }
8
9 function outputDecryption(message, key)
10 {
11   document.getElementById('encryptKey').value = key;
12   document.getElementById('decryptKey').value = key;
13   document.getElementById('encryptInput').value = message;
14   document.getElementById('decryptInput').value = message;
15 }
16

```

The JavaScript files, assets, and CSS files used for the website are inside their respective folders to keep the files separate and organized.

3.2 Caesar Cipher Implementation

The way the Caesar Cipher works is by taking the users message and key and shifting each letter in the message right based on what the user has put for key. If the user's message and key are "abc" and 2, then the encrypted message would be "cde". There is a for-loop that goes through each character of the message and based on if it is a capital letter or not, it get its character code and adds the key to it. And to decrypt it, you do the same but subtract the key to each character code.

The figure shows two side-by-side web forms for the Caesar Cipher. The left form is for encryption, with a message input field containing 'hellosimon', a key input field containing '3', and an 'Encrypt' button. The right form is for decryption, with a message input field containing 'khoorvlprq', a key input field containing '3', and an 'Encrypt' button.

Figure 4: Caesar Cipher

3.3 Playfair Cipher Implementation

The way the Playfair Cipher works is by taking the users message and splitting the letters into pairs of 2, if there is an odd letter out, you add the letter 'x' to it. If there is a pair with the same letter, you then have to insert a 'x' between them. Then you create a 5x5 matrix grid that is made of the key phrase and the alphabet language with the exception of the letter 'j' (if message contains the letter 'j', it will be replaced by the letter 'i'). You find where each pair of letters

are positioned in the key matrix, and change their positions depending on three cases. First case is if the two letters appear on the same row in the key matrix, then replace each letter by the letter to the right of it (it will overlap to the left side if needed). Second case is if the two letters appear in the same column in the key matrix, then replace each letter by the letter below it (it will go back to the top of the key matrix if needed). Last case is if the two letters are at two opposite corners that form a rectangle, then replace each letter by the letter that forms the other corner of the rectangle which lies on the same row as each letter.

To decrypt the message the same steps as encryption are repeated with the exception of the first and second case, in which you take the letters to the left and above respectively. Must also remove any 'X' that was in the encrypted text.

The figure shows two side-by-side web forms for the Playfair Cipher. The left form is for encryption, with a message input field containing 'hellosimon', a key input field containing 'cipher', and an 'Encrypt' button. The right form is for decryption, with a message input field containing 'ecspgsqpgtlz', a key input field containing 'cipher', and a 'Decrypt' button.

Figure 5: Playfair Cipher

3.4 Rail Fence Cipher

The way the Rail Fence Cipher works is by taking the users message and splitting that message across lines in a "zig-zag" fashion. Then the encrypted message is formed by reading each line in order. The number of lines depends on the user's key. This implementation is not complete, it will not work if the key is bigger than the length of the message.

The figure shows two side-by-side web forms for the Rail Fence Cipher. The left form is for encryption, with a message input field containing 'hellosimon', a key input field containing '3', and an 'Encrypt' button. The right form is for decryption, with a message input field containing 'hooelsmnl', a key input field containing '3', and a 'Decrypt' button.

Figure 6: Rail Fence Cipher

3.5 Simon Wells Cipher

The way the Simon Wells cipher works is by taking the users message, and just like the Playfair Cipher, splits it into pairs of 2. There is no need for the letter 'x' to be inserted between letters that are the same for it does not matter in this case. Then just like the Playfair cipher, you find where each letter is positioned in the key matrix that is made out of the key phrase the user typed in. However, unlike the Playfair cipher, we find the row and column of each letter that is positioned in the key matrix and take those numbers. You are then

left with numbers that for each pair of numbers represents a letter in the key matrix. Then each number gets an amount added depending on the second key the user types in which is numeric.

To decrypt you take away the amount added to each number and then find what letter each pair of number represents in the key matrix. In each pair, the first number is the row, and the second number is the column.

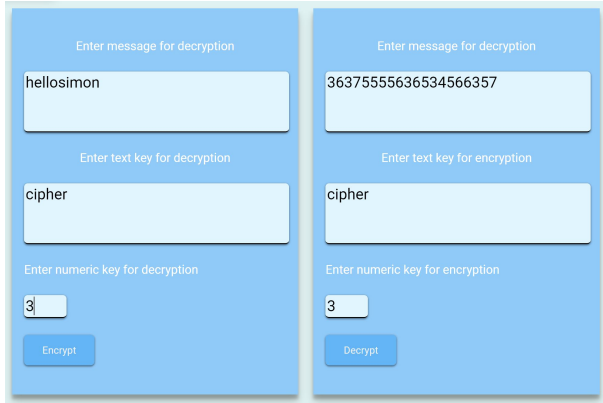


Figure 7: Simon Wells Cipher

4 Critical Evaluation

4.1 Comparison Against The Requirements

The minimum requirements of this assignment involved using HTML, CSS, and JavaScript to create a website that incorporates ciphers. There was to be no use of any external libraries or frameworks, and it must at least include an index.html page, a design.html page, and an additional html page for each cipher that is implemented.

The requirements for the amount of ciphers incorporated in the website was at two, but this website incorporates four different ciphers. There was no requirement for how complex the ciphers should be, however, some ciphers included will be more complicated than others.

There was no mention of developing a responsive version of the website, however it was a worthy addition for it adds on the overall style of the website.

As for the evaluation of the website as a whole, it inherits from Google's Material Design philosophy. As far as Design is concerned, it will be a design that is not foreign to users, and allows for ease of use. There is nothing in the website that yells out exotic, and there were careful design choices to focus more on usability and readability.

4.2 Possible Improvements

Since it is a simple website with not much to do, there aren't many improvements to be made. One improvement would be to make it so when you click on the button to slide in the navigational bar from the left, the button also slides inwards and disappears and only slides back out when the navigational bar is closed. Another improvement to the side navigational bar would be to make the text for the links to not re-size as

the bar opens and closes. Having a little animation queue when you click on any button would be an improvement on design. A welcomed improvement on the website would be with the implementation of the Rail Fence cipher. The cipher works as long as the key the user inputs is less than the length of the message. The improvement would be to fix this issue and have it work regardless of message length. There could have been more information on each cipher. Other tweaks that could make the website better, would be in a style sense.

5 Personal Evaluation

Before this module, I hated web, and now I hate it less. I had a little understanding of how Web technologies worked, but no real practical experience until this assignment. This assignment has taught me to how to design a website from scratch, and I learned that designing a website stylistically isn't so different from how programmers write their code. Everything is done with design in mind.

Some of the challenges I faced through this course work had to do with mostly with design and CSS. Since it was all fairly new to me, I had to learn how to use CSS. It wasn't a smooth experience for it involved a hefty amount of background reading, trial and error, and planning. The developer tools for the browser was at first challenging, but once I figured it out, it helped me a lot with this assignment. I could debug and view all element style properties with ease, and that made writing JavaScript and CSS more bearable.

This assignment was a very good starting point to web development. This assignment allowed me to research with only depending on myself. I feel good about this website, and am waiting for what lies next.

6 References

- [1] <https://material.io/> - Google's Material Design
- [2] <https://stackskills.com/> - Stackskills (I have a free course on web development)
- [3] <https://www.w3schools.com/> - W3Schools
- [4] <https://en.wikipedia.org/wiki/Cipher> - Wikipedia
- [5] <https://translate.google.co.uk/> - Google Translate
- [6] <https://www.braingle.com/brainteasers/codes/index.php> - Braingle Ciphers