Web Technology Coursework 1 Report

Jonathan Binns

40311703

Introduction

In this task the goal is to create a website that allows the user to encipher and decipher text in a choice of different ciphers. It should have a rewarding user experience that is easy to navigate and easy to both enter and retrieve the messages from. It should be achieved by having multiple files for each web page, a .HTML file which dictates the layout and text of the page, a .CSS file that dictates the styling of the page and finally a .js file that contains any JavaScript methods needed in the website.

The two ciphers I decided to impliment are Bacon's cipher and the Rail Fence cipher. Bacon's cipher was invented by Sir Francis Bacon around 1576 to 1597 while he was in Paris (Dawkins. 2016). The main principle of this cipher is that each letter in the alphabet is given a 5 letter code made up of two values, for example 'b' becomes 'aaaab'. The main reason I chose this cipher is that it became the basis of important ciphers such as Morse Code and it was also the basis for how alphabetic characters can be represented in binary (Dawkins. 2016). The second cipher I chose was the rail fence cipher. It is an example of transposition or route cipher which was popular during the early history of cryptography (Simmons. 2011). The cipher works by splitting the message into a known number of parts, known as the key. The message is then split into these parts based on where each character is in the message, for example 'abcd' becomes 'acbd'. In order to decode the message the enciphered message would be written diagonally in a grid, revealing its message. I chose this cipher because it's doesn't follow a standard cipher structure, the letters are not replaced by another letter the entire string is rearranged. Testing my skills of working with strings and arrays of characters.

Software Design

The first place I started when designing this website was comint up with a list of requirements for how it will function and how it will look. This allows me to have a good idea of what my website will look like before I have written any code. My first requirement is that the website should be easy to navigate, I plan on ensuring this by making the website as minimal as possible, it should only have the features and layout necessary for enciphering and deciphering text. This stops the website from becoming too complex and hard to navigate. The second requirement for the website is that it should encipher and decipher text in two different ciphers. Adding this as a requirement ensures that the website is functional for its most basic of tasks and that it completes the main goal of this assignment. My final requirement for the website is that it should be pleasing to the eye. All text and information presented to the user should be easy to read and understand. This leans into making my website easy to navigate, as any links to different pages should be easy to find.

Add navigation diagram

As my navigation diagram shows I plan on having three pages in my website. A homepage, a page for Bacon's cipher and a page for the rail fence cipher. This keeps the site from having too much information on one page and thus keeps it simple to use. My home page should have links to the other two pages, this will come from having a area the user can click to take them to their desired cipher. The pages from both the rail fence cipher and Bacon's cipher should link to each other in order to let the user switch ciphers with one click. Finally both cipher pages should link to the home page in order to make sure all pages are accessible from each other.

Add Wireframe for homepage

I decided to keep the homepage simple and just use it to display information about the ciphers the user can choose. My plan is to have the background of the name of the cipher act as a link to the ciphers page. In order to make sure the user knows what they are about to click I will have the background turn a shade of grey while the mouse is over the link. The background for all pages will be an off white with the text being a dark grey to reduce overall contrast slightly and make the text easier to read.

Wireframe for Bacons

My layout for both Bacon's cipher and the Rail Fence Cipher are mostly the same, ad they have to achieve the same function and keeping a website consistent is an good way to keep it user friendly. The first element is a big text box where the user can add text to be either enciphered or deciphered. Once a button is pressed the text will be displayed in a text box beneath the button denoting what function has been applied to the text. Beneath that is the same information as was presented on the homepage telling people a little bit about the cipher. In order to implement Bacon's cipher I plan on splitting the input string into its individual letters then replacing them with their corresponding code and adding them to an output string. For decoding this cipher my plan is to split the input string into substrings of five characters then take those strings and replace them with their corresponding letter of the alphabet.

Wireframe for railfence

My design for the Rail Fence cipher is mostly similar to my design for Bacon’s cipher, with the addition of another text output area where the enciphered text can be displayed in a zig zag pattern showing how the cipher can be read. My implementation of this cipher will split the input string into three substrings. The middle string will have around twice as many letters as the top and bottom as it naturally occurs more in the cipher. Ideally, I can do this inside of one loop, taking in the input string and sending the characters to one of 3 others. For decoding on the other hand, I will need to calculate a formula that will tell me how many characters appear in all of the strings so I can ‘rebuild’ them back into one string in the correct order.

Implementation

Homepage implementation and explanation\\Bacons implementation (show code), explanation \\ Rail Fence implementation (show code), explanation

Evaluation

comparison Against the Requirements

Improvements

Personal Evaluation

References

Dawkins, P. (2016). Baconian-Rosicrucian Ciphers, An introduction to the cryptography used by Francis Bacon and the Rosicrucian-Freemasonic fraternity. Retrieved From: <https://www.fbrt.org.uk/pages/essays/Baconian-Rosicrucian_Ciphers.pdf>

Simmons, Gustavus J. (2011). Transposition cipher. Encyclopaedia Britannica.

Retrieved From: <https://www.britannica.com/topic/transposition-cipher>