

Coursework Report

Sean Pickles

40318409

Web Technologies (SET08101)

Introduction:

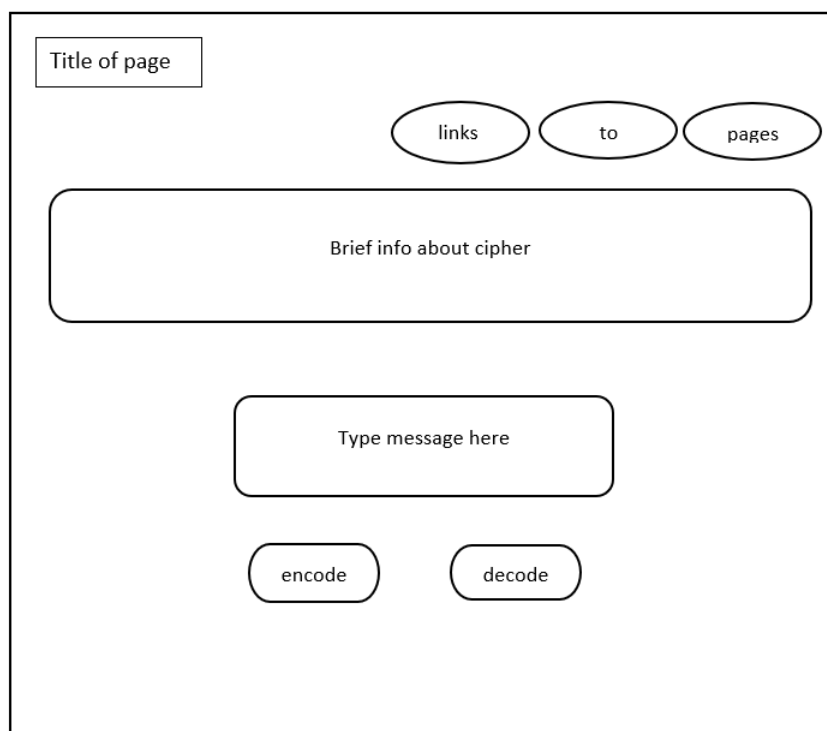
The aim of this assignment was to enable users to encrypt and decrypt messages using various ciphers.

I chose the Caesar cipher as it widely known and relatively easy to both understand and implement. I then chose Atbash because of its simplicity as a way of encryption.

As a way of helping me with this coursework I learnt most of what I needed through reading several W3schools tutorials and assorted other resources. As well as using the materials provided and recommended by the lecturer Simon Wells.

Software Design:

I already had an idea of what I wanted the layout of the website to look like before I started. It was influenced to look like browsers such as Google or Bing as they are both simplistic and aesthetically pleasing.



For each cipher page; there is a brief overview of what the cipher is and does – I have also included an external link to more background information. A navigation bar along the top right of the page to cycle through each page. A place for the user to type their plaintext message and buttons to both encode and decode using the selected cipher.

I have mostly been able to follow this structure with very small changes. I chose to use an image as the background for each page because I wanted it to be consistent throughout. I chose the font for most of my text to be courier because it's usually associated with programming, computing in general – fits in with the theme of the task.



Implementation:

Each page follows this basic structure: each one has its own html files for navigating back and forth between all the pages and one single CSS file to contain all the styling for each.

Caesar Cipher –

At first, I concentrated on only trying to code ROT13 to see if it worked. After that I was able to make sure that all shifts (ROT 1-25) were available to the user by the end.

I was able to implement the different shifts using ascii characters – having to find the ascii code that corresponded to the letter, then adding the number of shifts to it - instead of using an actual alphabet within an array.

Once I had the encrypt part working, decrypting it was easy because I only had to switch the pluses (+) and minuses (-) around for the shifts.

Caesar Cipher

HomeCaesarAtbash

In cryptography, a Caesar cipher (shift cipher etc...) is one of the most known encryption techniques ever used. It's a type of substitution cipher where each letter in the plaintext is replaced by a letter corresponding to a certain number of letters shifted up or down in the alphabet. There are total of 25 possible shifts with this cipher.

[More background info](#)

Enter message here:

Sean

13

Frna

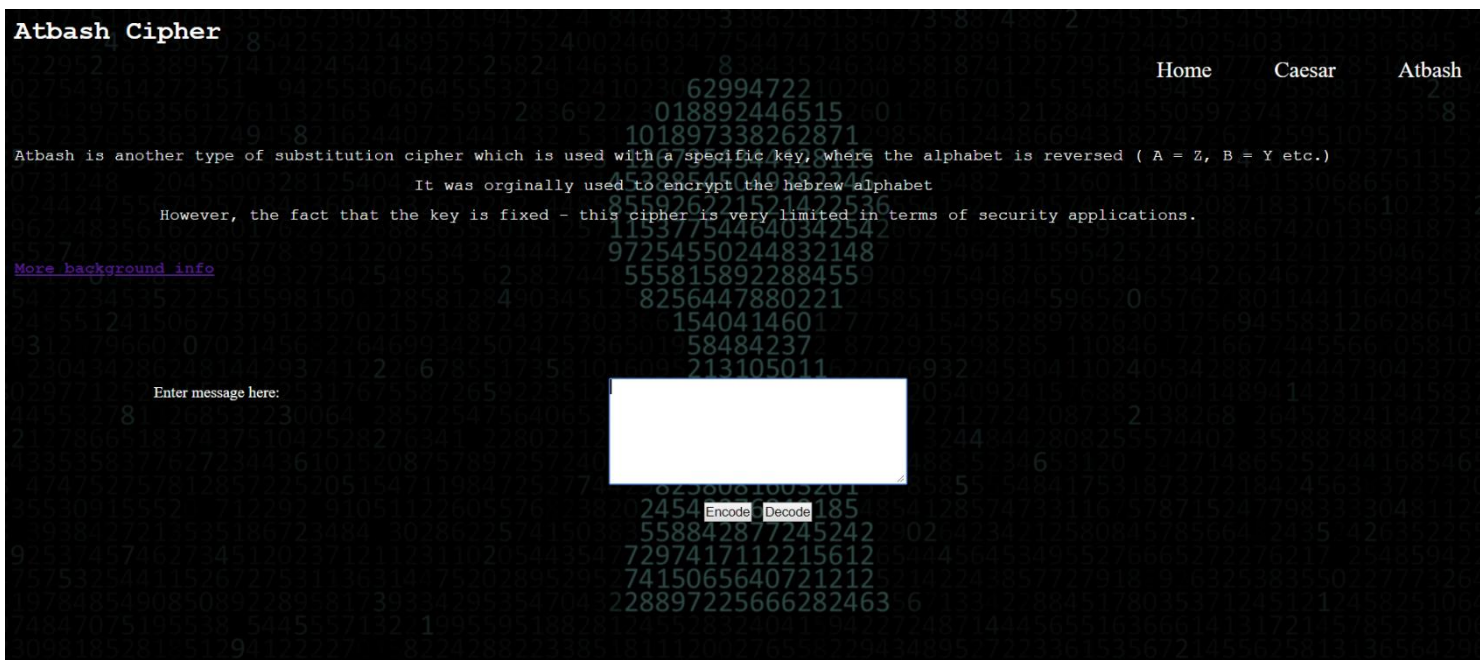
Encode

Decode

Atbash Cipher –

The Atbash was very simple to implement because the key is just using the original and reversing it (A=Z etc.).

I took a slightly different approaching to implementing this cipher. As it was a very small function, I decided to embed it within the Atbash html file. I did this because every letter in the alphabet has the same corresponding cipher key throughout there was no need for a separate decrypt JavaScript file.



Critical Evaluation:

The specification of this task assignment was to implement and design a website – with the use of HTML, CSS and JavaScript - that would enable users to encrypt and decrypt their own messages using a variety of different ciphers.

I think in terms of learnability; this site is very simple and easy to navigate and get the job done quickly. I also consider this website to be efficient as the text is very easy to read and the encryption/decryption process is very fast. Therefore, the website meets the requirements.

However, like with everything, there is always room for improvement – even if a website meets a certain specification, adjustments can be made to improve upon them.

I think in the future, another page could be added which would provide links to pages that are related to sites for those who are interested in learning more about cyber-security, and some videos detailing more about the ciphers themselves.

In regard to the design of the website, all the ciphers could be available on the one page as to make the navigation more linear and making it even easier to navigate. Instead of using one image of the background image for every page, different colour schemes could be used together to make the overall appeal and look of the website more inviting and exciting for the user. More JavaScript and HTML could be added to add more movement to the navigation of the website, as well as making more fun.

Personal Evaluation:

Before starting Web Technologies, I had a basic understanding of what HTML and CSS were and how they worked. But after starting this module and this task, it has opened my eyes to how much HTML, CSS and JavaScript can do when put together.

I had to do a bit a self-learning in order to better understand how to handle this task. I used a variety of resources at my disposal such as W3Schools and the lecture/lab materials provided. However, I do regret not taking the chance to use books from the library in order to bolster my understanding. I also think that I could have implemented more ciphers for my website which solidify my knowledge of JavaScript even more.

References

<https://www.youtube.com/watch?v=M15LVmGe8-w> (startup for Caesar cipher)

<http://practicalcryptography.com/ciphers/classical-era/>

<https://www.w3schools.com/html/default.asp>

<https://www.w3schools.com/css/default.asp>

<http://www.asciitable.com/>

<https://pixelz.cc/wp-content/uploads/2017/11/tech-security-illustration-code-and-key-hole-uhd-4k-wallpaper.jpg>

https://cdn-images-1.medium.com/max/1600/0*wDm8-tNnnBkwd3Q5.jpeg