Edinburgh Napier UNIVERSITY

# Coursework

Ovidiu-Andrei Radulescu
40283288@live.napier.ac.uk
Edinburgh Napier University - Web Technologies (SET08101)

## 1 Introduction

**Cryptography** is the use of codes and ciphers to protect secret messages. It began thousands of years ago and in the beginning it was almost synonymous with the art of writing and it has evolved ever since with the need of protecting sensible information to what we all know today. This assignment tackles the history of cryptography by building a website that encompasses a brief history, explanations and three fully working ciphers that can be used for encrypting and decrypting messages.The ciphers presented in the website are Caesar, Vigenere and Hill, which showcase the evolution of ciphers from the very rudimentary Caesar cipher to the fairly modern, early 20th Century, Hill Cipher.

**I have chosen** these ciphers as they are all a step in the evolution of the same mechanic, shifting the letters, from the simple Caesar, which shifts the whole alphabet at the same time a certain number of positions, then to Vigenere who shifts a group of letters based on they key and then to Hill which uses matrices to encode a text with a key.

**The main source of documentation** has been Crypto-Corner [1] which has been of immense help in making the Hill Cipher functional by having step by step guides in how its matrix encryption works. Other sources have been TutorialsPoint [2] in helping me making sense of how the ciphers started and evolved, and of course, Wikipedia [3] for everything I wanted to know about a specific cipher, or for just simply helping me remember what a matrix inverse was.

## 2 Software Design

**I started out** on the assignment by making a few sketches on paper on the first day, which had a big impact on the layout of the page. I then set out on making a list of things I wanted to implement in the website.

- Navigation Bar
- Parallax Images
- Buttons with animations
- A nice minimal style
- 3 Ciphers at least

**It all started with** the pages I will write. I sketched on paper the initial draft that had an "index", "history", "about" and a number of ciphers. That proved to be excessive, as the index and history pages merged into one by the time I started writing the html code. The about page quickly proved pointless, as there was nothing much to write in it except my name and the module, and so the about page was replaced by the design page.

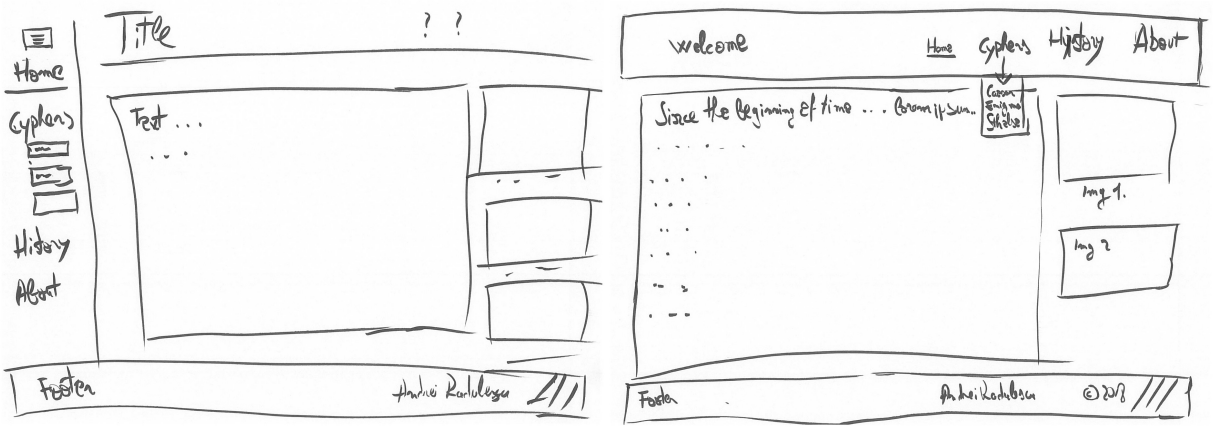


Figure 1: **Two Layout Sketches** - A vertical NavBar design and the design that inspired the website

**The conclusion** of the sketches is that I decided to go with a very minimalist design, and as a result there are only 3 distinct pages: the homepage, design and ciphers. I made a simple diagram(pictured below) that showcases the relation between the pages and the way a user might navigate it, by first reading the contents of the homepage, then making their way to testing the ciphers or looking at the design page.

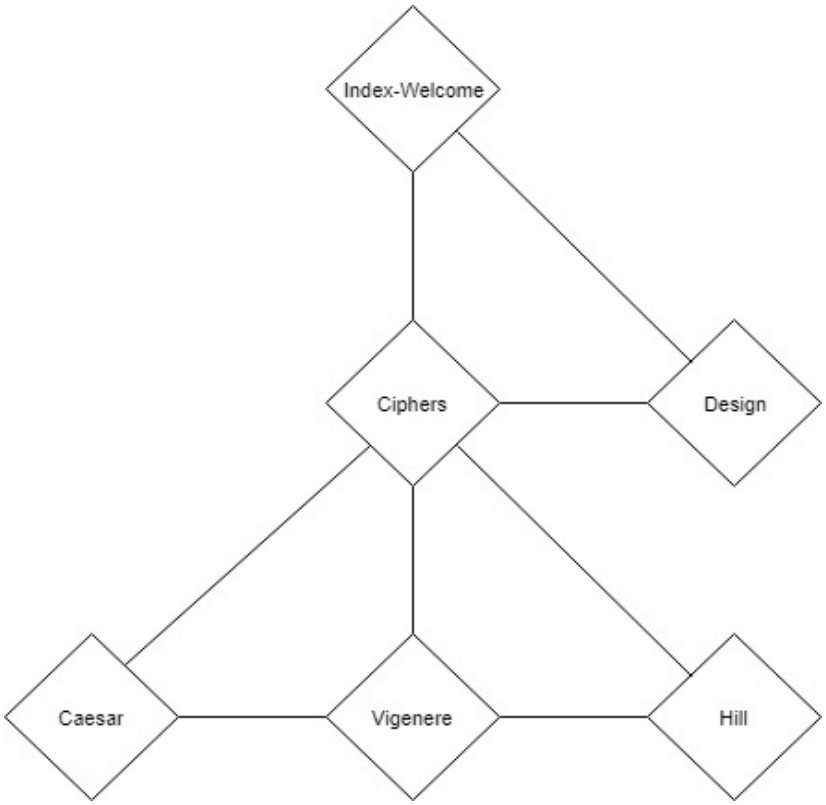


Figure 2: **The navigation diagram**

**The way** I approached the assignment was by doing one part(HTML, CSS, JavaScript) at a time. I would start by writing the basic html of the index page: the list of hyperlinks to the other pages, titles, paragraphs. Then with CSS, adding images, card elements, button animations and after all that I would start writing the JS for the ciphers, as they required at least a working web page for troubleshooting.

# 3 Implementation

**I drew** a lot of inspiration from Android and Apple websites, as I've always been a fan of minimal design. Then with the help of CSS, I transformed the ugly html elements into a navigation bar with a drop-down for the cipher pages then added several images that had a parallax effect(as you scroll the page the image remains static in it's place, creating the illusion that the text is scrolling on a different scene in front of the image, like watching the outside of a glass elevator). I then turned the index into a general template, to which I added the necessary elements for the cipher pages: a text box for input, a text field for key, buttons for the encryption and decryption functions, as well as a field for the output. This template page is the design page now and showcases all of the elements used in the website.

**I then** started making the cipher pages, the most notable differences being the personalised descriptions, instructions and a different type of key field for the Caesar Cipher, because the Caesar Cipher has a fixed amount of 26 possible key shifts. During this time, a friend of mine who has made websites in the past told me it is good practice to make a folder for each html page, creating in the process a way of naming all of them 'index', which would look nice in a web address because it would display as "website.com/cipher" as opposed to "website.com/cipher.html" and that seemed like a sensible idea that was easy to implement and very useful.

**With the design finished** I started working on the JavaScript for the Ciphers. As I have never used JavaScript before the difficulty of the ciphers and my ability to make them was very [ironically] inversely proportional, meaning that as the ciphers became harder, the time it took me to figure the algorithms was shorter. JS proved to be interesting and easy to use, but if I were to complain about one feature it would be the unified variable types. JavaScript only uses a general type called "var", which seems all nice and easy, until it won't work and suddenly an integer becomes it's string counterpart (and they are not the same value as it turns out).

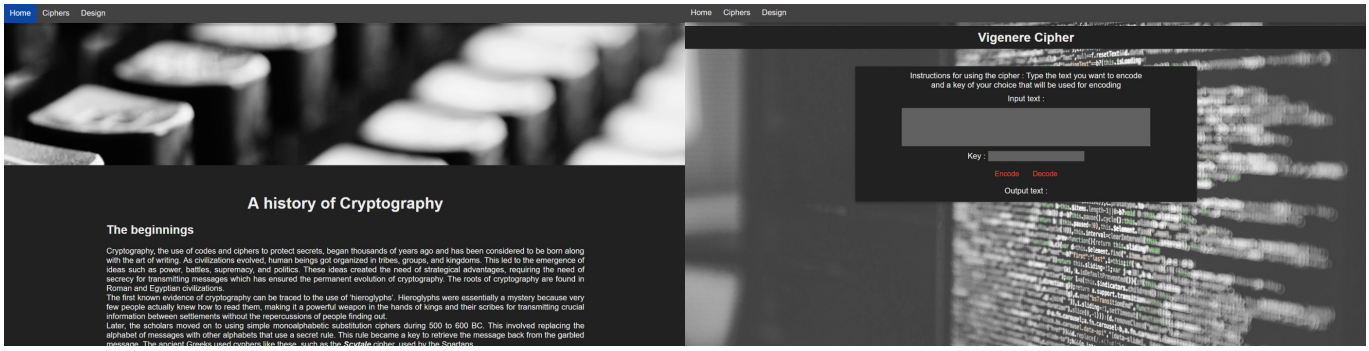


Figure 3: **Screenshots** - Homepage(left) and The Vigenere Cipher(right)

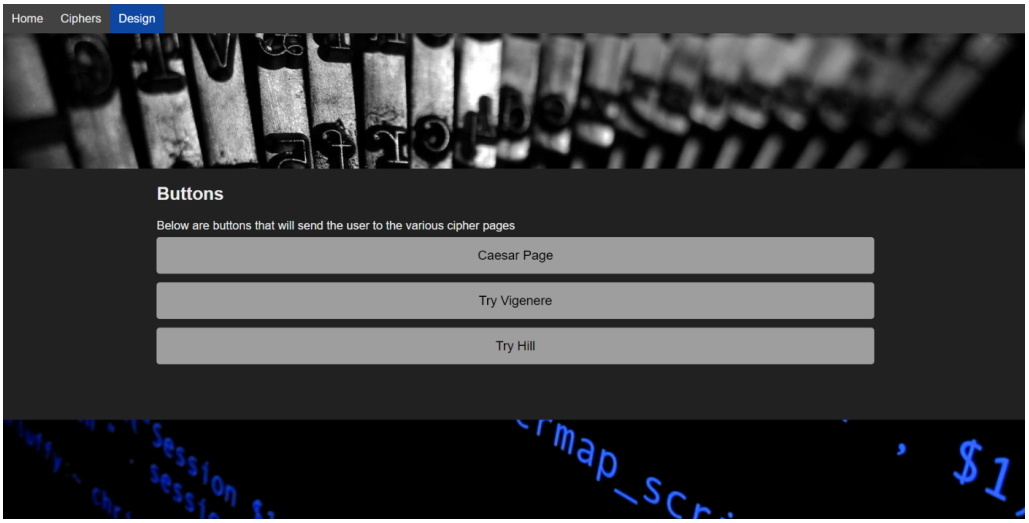


Figure 4: **Screenshot of Design Page** - Showcases buttons that send you to the cipher pages

# 4 Critical Evaluation

**I started this project** with the goal of making a website that was pleasing to look at, functional, and all in all useful. The above points are a testament that the goal was achieved. I have also asked people I know from outside the School of Computing for testing and feedback and all of them had no problems understanding how to navigate the website or in using the cipher programs. The people who didn't know about ciphers beforehand found the website very interesting and a curious glimpse behind their day to day websites and their privacy.

**I am pleased with the design** of the website, but if I had more time I would have wished to improve on it by making it mobile-friendly and experiment with the original idea of a left vertical Navigation Bar that had a hide function. I liked sticking to the limited colour palette of black with blue accents and images that gave it a spark of colour, which I thought fitted very well with the theme of historical ciphers, a very serious subject. I would like to experiment with more vibrant colours, like the ones on most Google-made websites, as those websites seem to give the user a more friendly feeling of familiarity.

**The ciphers** were of course at the main centre of the website. The information given about ciphers, their history, evolution and different types and variants is not long but engaging as to not bore the reader but keep them interested further. The cipher pages only showcase the cipher program with instructions on how to use the cipher as to not distract the user from the main reason of visit. The ciphers themselves are interactive, letting you choose the key you want your message to be coded in. One point I would have liked to improve here would have been introducing the use of a custom alphabet the user could create, as opposed to the standard A-Z alphabet.

**The website's size** was kept at a reasonable small size of only 5 pages, including the design page. I have discovered a lot of things and curious trivia about ciphers during the research such as the first book written by an Arab mathematician about breaking the ciphers at the time, which I would have loved to share on the website, but they didn't seem to fit with how the website was shaping up so they weren't included. I have always been fascinated by the infamous Enigma machine, and I wanted to create an Enigma program but that proved incredibly difficult to do in JavaScript.

# 5 Personal Evaluation

**I have learnt** a great deal about the structure of a website, about the user experience, and most importantly, the difference between margin and padding. Although I have first learnt HTML a very long time ago, I have never used CSS very extensively, this assignment helped me a lot with understanding CSS better and making the html code much more cleaner by having the style in a different place, ready to be used multiple times.

**JavaScript** has been a central piece of the website, but it was quite stressful in the beginning, trying to make it work for the simplest tasks of just printing logs to the console all the way to complex matrix calculations. When I decided to write the Hill cipher, Crypto-Corner proved to me an indispensable help as it had every detailed step in encoding and decoding using matrices as well as a working example that proved of an immense help in debugging the program, because the math was so complicated, the Hill cipher took the most part of this assignment, but the end result proved to be worth it and I am very proud of it. The only disappointment I had is when I realised that, by using matrices to encode, and therefore using inverse matrices to decode, not all keys would be compatible, since not every matrix has an inverse, and that turns out to be common in a 2x2 or 3x3 matrix that can only contain numbers between 0 and 25(every number corresponds to a letter in the alphabet, starting with A—0), but there was nothing I could do as that's how the cipher operated.

**The unexpected part** of this assignment was LATEX. I expected LATEX to either be easy to use or something I wouldn't want to use again. I was very wrong about both of those things. The first page of this document took a very long time to write as I tried various styles and options and everything under the sun to make two images show up on the same row. But then I realised, I can merge them into one picture. From there on it has been smooth sailing, as I have already gotten used to the various elements of LATEX and I will definitely write everything in LATEX from now on and I will continue to pass on to others the knowledge and beauty that is LATEX.

# References


[1] D. Rodriguez-Clark, "crypto.interactive-maths.com,"

[2] Tutorials-Point, "https://www.tutorialspoint.com/cryptography/index.htm,"

[3] Wikipedia, "https://en.wikipedia.org/wiki/History_of_cryptography,"