**Computer Science Project**

**Encryption software**

**Joseph o Elliott (5049)**

2020-2021

# **Introduction:**

Cyphers have been used for 1000s of years. The earliest know cypher was found in the tomb of Khnumhotep II who lived around 1900 BC in Egypt. This was symbol replacement encryption meaning a key was needed to understand the text. Similar types of encryption have been further used throughout Ancient Greece and Rome for primarily military purposes. One of the most know cypher of this style is the Caesar Cipher named after Julius Caesar. However this style of encryption was broken around 800 AD by Al-Kindi a mathematician who developed a technique of frequency analysis to determine the key used to shift the text.

Thomas Jefferson theorized a way to encrypt information using a wheel cypher in around 1790 however this cypher was not implemented until 1917 when the US military independently developed the M-94 using the theorised wheel cypher. This idea was then taken during WW2 where the axis power used a more advanced version of the M-94 called the enigma machine to encrypt their communications. However even this was later cracked by Alan Turing.

In the modern world encryption is used almost everywhere as it provides a very simple and effective way of securing communication and commerce over the internet. The advent of modern computing has had a massive impact on encryption with 56bit encryption going from being more than adequate to inefficient within the Morden world.

However many people today have very little idea behind how encryption works or the types of encryption found in the Morden world. It is this I seek to change with this project in creating a programme that can be used to encrypt and decrypt using various methods. This programme will also provide information about the encryption such as where it can be found today or historical information about it.

Encryption is used in everything in the Morden world from most websites with HTTPS and WhatsApp to bank transfers. Therefore, it is incredibly important people understand the basics of how encryption works and how secure different types of encryption are. To do this I have created an application to demonstrate how different types of encryption work. To this end I am planning on using a series of more basic cyphers to teach how encryption works and then some more advanced encryption methods to show how encryption works in the Morden world. These methods are:

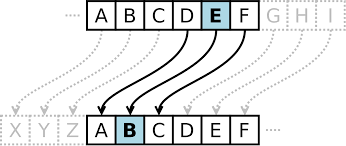
Caesar cypher, named for Julius Caesar who used this cypher to encrypt messages of significant military importance. This encryption works by shifting a message by a set amount of characters either left or right.

Figure - Caesar cypher

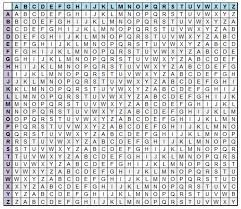
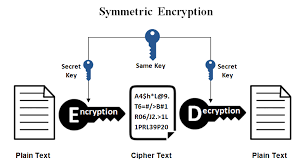


Figure - Vigenère Grid

Vigenère cypher, this is a cypher based of the Caesar cypher. However this cypher increases security greatly by shifting with a key instead of a pre-defined amount. The cypher works using the Vigenère grid (Fig 2). You start by laying your message out with you key beneath it. Then you take the first letters of both putting the key on the Y – axis of the graph and the sentence to be encoded on the X – axis and then find where they intersect getting your encoded character. This cypher demonstrates increased security from using a key instead of a shift method.



Symmetrical key, this is one of the most commonly used encryption methods used today as it provided some of the best security. This is going to be used to demonstrate how encryption works within the internet today.

Figure - Symmetric key Encryption

# **Design:**

UI design:

**EXIT**

**Enter**

**Help**

This will be the main box in where information will be displayed to the user

High level Flowcharts:

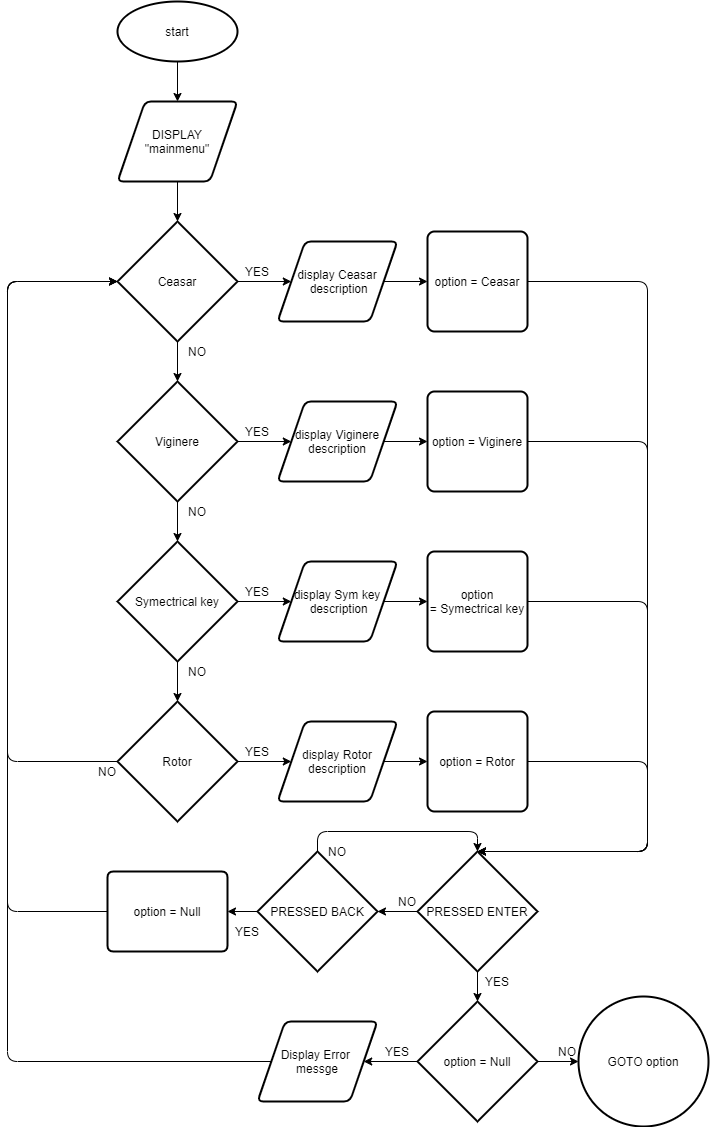


Figure - High Level Flowchart of Main menu UI

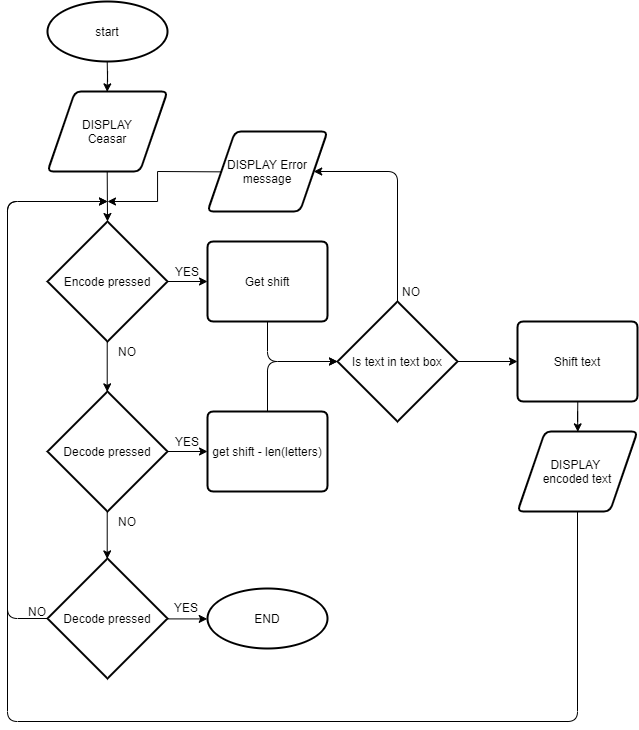


Figure - High level Flowchart of Caesar UI