FINAL REPORT

Animating Security Concepts

Author: Lara Ashford
Student number: 1718561

Supervisor: George Theodorakopoulos
Moderator: Parisa Eslambolchilar
Module Number: CM3203
Module Title: One Semester Individual Project
Credits: 40

Abstract

Within this report I will detail how I developed a series of interactive animations covering security concepts that are intended to aid people wanting to learn about the vulnerabilities of cyber security and how cyber security works. This report will show the process I used for my background research, design and implementation stages. I will detail my research into how human learning is improved through various different methods and explain the rationale for the decisions I made and the iterations that took place with the coding of my animation. I will then report my results and evaluation of the animations I created. Finally, I have highlighted areas for potential future enhancements to develop this project further.

Acknowledgements

I would like to thank my supervisor George Theodorakopoulos for supporting me through the duration of this project and offering both guidance and constructive criticism when necessary. Our regular meetings helped me to keep the project running on schedule, through a very challenging time of the Coronavirus pandemic and balancing work on my dissertation with numerous graduate job applications.

Table of Contents

ABSTRACT 1

ACKNOWLEDGEMENTS 1

TABLE OF FIGURES 4

1. INTRODUCTION 5

1.1 PROJECT AIMS 6
1.2 PROJECT OBJECTIVES 6

2. PROJECT BACKGROUND 7

2.1 LITERATURE REVIEW 7
2.1.1 WHAT IS ANIMATION? 7
2.1.2 WHY LEARN THROUGH ANIMATION? 8
2.1.3 INTERACTIVE LEARNING 10
2.1.4 COLOUR PSYCHOLOGY 11
2.1.5 RETRIEVAL BASED LEARNING 11
2.1.6 OTHER EDUCATIONAL ANIMATIONS OUT THERE 11
2.2 BACKGROUND MATERIAL 16
2.2.1 PUBLIC-KEY CRYPTOGRAPHY AND RSA 16
2.2.2 RSA 18
2.2.3 DIFFIE-HELLMAN 19
2.3 HUMAN COMPUTER INTERACTION 20

3. SPECIFICATION AND DESIGN 21

3. 1 USER PERSONA 21
21
3.2 REQUIREMENTS 22
3.2.1 MUST HAVE REQUIREMENTS 22
3.2.2 SHOULD HAVE REQUIREMENTS 22
3.2.3 COULD HAVE REQUIREMENTS: 23
3.2.4 WON'T HAVE TIME REQUIREMENTS: 23
3.3 SYSTEM STRUCTURE 24
3.4 DESIGN DECISION OF JAVASCRIPT MODULES 25
3.5 USER INTERFACE DESIGNS 25
3.5.1 HOMEPAGE 25
3.5.2 OVERVIEW OF MESSAGE EXCHANGE, KEY EXCHANGE AND MAN IN THE MIDDLE TEMPLATE PAGE 26
3.5.3 MATHEMATICS EXPLANATION TEMPLATE PAGE 27
3.5.4 FLASHCARD'S PAGE 29
3.6 ANIMATION OVERVIEWS 30
3.6.1 MESSAGE EXCHANGE OVERVIEW 30
3.6.2 MESSAGE EXCHANGE MATHEMATICS 30
3.6.3 DIGITAL SIGNATURES MATHEMATICS 30
3.6.4 KEY EXCHANGE 30
3.6.5 MAN-IN-THE-MIDDLE ATTACK 31

3.7 USER JOURNEY 32
3.8 USE CASES 33
3.9 RISK ASSESSMENT 34

4. IMPLEMENTATION 35

4.1 HOMEPAGE 35
4.2 MESSAGE EXCHANGE ANIMATION 37
4.3 MESSAGE EXCHANGE WITH RSA MATHEMATICS & DIGITAL SIGNATURES WITH RSA MATHEMATICS 38
4.4 FLASHCARDS 44
4.5 CHALLENGES FACED AND TECHNIQUES USED 46

5. RESULTS & EVALUATION 48

5.1 MOSCOW REQUIREMENTS EVALUATION 48
5.2 TEST CASES CHECKING FUNCTIONALITY 49
5.3 USER TESTING 55
5.4 EVALUATION 55

6. FUTURE WORK 56

7. CONCLUSIONS 56

8. REFLECTION OF LEARNING 57

1. APPENDICES 58

12. REFERENCES 61

Table of Figures

Figure 1 - Problems with animations and how to fix them (Malamed, 2016)[x] 9
Figure 2 Shift Disruptive elearning (shiftelearning, 2021)[xv] 11
Figure 3 Existing animation on Public-Key Cryptography (Simply Explained, 2017)[xxiv] 12
Figure 4 - Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv] 12
Figure 5 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv] 13
Figure 6 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv] 13
Figure 7 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv] 14
Figure 8 Interactive learning tool example (R2d3.us, 2019)[xxviii]. 15
Figure 9 Interactive learning tool example (R2d3.us, 2019)[xxviii]. 15
Figure 10 Interactive learning tool example (R2d3.us, 2019)[xxviii]. 15
Figure 11 Terminology Related to Asymmetric Encryption (Stallings, 2017)[xxxi] page 285 16
Figure 12 Encryption Process (Stallings, 2017)[xxxi] page 287 17
Figure 13 Decryption Process Stallings, 2017)[xxxi] page 288 17
Figure 14 Applications of Public-Key Cryptosystems (Stallings, 2017)[xxxi] page 292 18
Figure 15 Key Generation, Encryption and Decryption (Stallings, 2017)[xxxi] page 297 18
Figure 16 Encryption and Decryption (Stallings, 2017)[xxxi] page 297 18
Figure 17 Diffie-Hellman (Stallings, 2017)[xxxi] page 315 19
Figure 18 User Persona 21
Figure 19 File Structure 24
Figure 20 Site Map 24
Figure 21 Home Page UI Design 25
Figure 22 Timeline animation UI Design 26
Figure 23 Mathematics UI Design 27
Figure 24 Flash Cards UI Design 29
Figure 25 Homepage 35
Figure 26 Rotating Button 36
Figure 27 Button faces code 36
Figure 28 CSS for rotating button 36
Figure 29 CSS for rotating button 36
Figure 30 Message Exchange animation 37
Figure 31 Code of controls on animation 37
Figure 33 Movement of the animation 38
Figure 32 Creating a timeline code 38
Figure 34 Digital signatures animation 39
Figure 35 Code to make text clickable 40
Figure 36 Plotting of path in code 41
Figure 37 Code showing each movement in the timeline 41
Figure 38 Public Key starting its route 41
Figure 39 Public Key later on in its route 41
Figure 40 SVG Path Editor 42
Figure 41 Code of button creation 42
Figure 42 User input box 42
Figure 43 Validation on User input 42
Figure 44 Second route created to send the Digital Signature 43
Figure 45 Validation on user input box and then mathematics replacing the correct numbers in html 43
Figure 46 Flashcards once clicked 44
Figure 47 Flashcard's page 44
Figure 48 Html code for each flashcard 45
Figure 49 Declaring a card in JavaScript 45
Figure 50 anime timeline function for each card flip 45
Figure 51 Inspect tool on browser 46
Figure 52 Using Preview to annotate images 46

1. Introduction

Modern society has dramatically changed in a variety of aspects since the development of technology. From the transformation of how people do their jobs, to developments of phones, the use of IOT devices and driverless cars. Most aspects of life have been, or are being, changed by technology, both positively and negatively. This project endeavours to build on these developments in technology to inspire student learning and education, creating a positive use of technology. Specifically, this project aims to solve one of the negative effects of technology that has been generated, namely a skills gap in cyber security.

Research has shown that 653,000 businesses (48%) have a basic skills gap and 408,000 (30%) have a more advanced skills gap. (GOV.UK, n.d.)[i]. This shows the current lack of knowledge in existing staff members but also that there is difficulty recruiting people into the field. The most desired roles that are in high demand are security engineers (18%), security analysts (13%), security architects (10%), security managers (9%) and security consultants (8%) (GOV.UK, n.d.)[ii].

Fundamentally, knowledge in cyber security is more important today than ever before as more and more of companies and individuals' systems and data are online, creating vulnerability to security attacks. This has resulted in a growing demand for increased awareness and understanding of security concepts and cryptography, as well as a requirement for more people to join the industry sector to combat the security vulnerabilities generated through the use of technology. This creates a clear need for more education in security both before people embark on their careers into the working world and to encourage more people to work in cyber security. This can be achieved by making the learning process more enjoyable with the aim of encouraging people to pursue a career in cyber security.

How humans learn, and educate themselves, has drastically evolved from solely the use of textbooks and libraries to having a wealth of resources online since the creation of the world wide web. The use of interactive animations is becoming more prevalent in education, as they are useful in keeping those learning engaged in the learning process and giving immediate feedback about the subject matter being taught. By creating an interactive animation tool user learning can be enhanced and potentially improved in an area that is a priority. Additionally, since the world has been plunged into the Covid-19 pandemic there has been a drastic switch to online learning thus creating this online animation can work towards helping those studying from home.

In this project, I will design and develop an educational web-based interactive animation for cryptographic concepts.

This project is important as it will help students to enhance their education through improved understanding and expand their knowledge of security concepts by having interactive elements to the animation. This will enable them to absorb the concepts by creating an experience that will promote the enjoyment of learning and stimulating an interest in the subject area. This project will utilise the developments of technology to create this tool for educational purposes addressing the growing need to educate people on both how security concepts work, and the need for them, due to the transition to online learning.

1.1 Project Aims

The overall aim of my project is to create a web-based interactive educational animation that will actively engage the learner and aid them in their education of cyber security knowledge.

Aims
1. Expand my technical knowledge on security concepts and encryption methods as well as my skills and abilities in the development and coding of interactive tools.
2. Investigate and understand what enhances a user's learning and understanding of concepts in regard to visual aids and why this improves learning.
3. Produce a web-based animation of security concepts for the intended target audience of university students who have a security module or element in their degree.
4. Identify the impact of the users understanding of the subject area before and after using this projects animation to ascertain if it enhanced their understanding.
5. Enhance students understanding of the chosen security concept
6. Detail and evaluate my findings in the final document of my individual project within this report to highlight the benefit of using animations within education and contribute to the improvement and development of modern learning.

1.2 Project Objectives

1. Research
1.1. Carry out research into different security concepts and encryption methods and decide on which to animate for this educational tool
1.2. Learn about the benefits of visual learning and what requirements are needed to be satisfied to generate better learning through animations
1.3. Explore the different programming languages, libraries and platforms are available to create an animation
2. Design
2.1. Research and determine a design methodology to use and establish if there are any proven design requirements/ frameworks of visual tools that have proven to enhance a user's learning experience
2.2. Design the animation, including the User interface Designs, description of interactive elements, use cases and user journey maps.
3. Implement the animation
3.1. Create the web-based animation using a chosen design methodology and programming languages
4. Testing
4.1. Use alpha testing initially and make any changes necessary from failed tests
4.2. Conduct functionality beta testing (user testing) to determine ease of use of the animation, navigation flow and other functionality conditions.
4.3. Carry out user testing to establish whether the tool enhanced users understanding of the subject area.
5. Evaluate and document
5.1. Collate all work and results into a final document
5.2. Analyse and evaluate the project's findings and determine a conclusion
5.3. Complete final report

2. Project Background

2.1 Literature Review

Upon first starting this project I undertook research into what an animation is and whether there is any evidence to support the concept that animations specifically improve people's learning and if I can use any of these features within my animation. Next, I researched the benefits of visual and interactive learning, as well as finding out what features of learning are needed to gain the most learning possible. Combining all of this together I intend to use this research to guide me in the making of my educational interactive animation to be able to educate the users on a security concept.

2.1.1 What is Animation?

Animation is defined by - (Oxford Languages, 2021)[iii]
"the technique of photographing successive drawings or positions of puppets or models to create an illusion of movement when the film is shown as a sequence."

Computer Animation is defined by - (Oxford Languages, 2021)[iv]
"the manipulation of electronic images by means of a computer in order to create moving images."

Types of animation

There are many types of animations, however these are generally classified into five key categories of animations (New York Film Academy, 2017)[v]

I. Cel (Celluloid) Animation

The first form of animation which entails an artist hand drawing thousands of images on transparent sheets known as "cels" that at are then placed in front of a coloured background and individually photographed. These images would be combined to play through the animation, which was first used by Walt Disney in the 1930s to make cartoons such as Tom & Jerry. (Alex Safavinia, 2020)[vi]

II. 2D Animation

Stands for two-dimensional animation which is created by two-dimensional images being rapidly sequenced to generate the like life illusion of something being in motion, It is similar to the traditional cel animation, commonly used with computer generated vector graphics. (www.dictionary.com, n.d.)[vii]

III. 3D Animation

Stands for three-dimensional animation which as the name suggests is created by having three-dimensional moving images. The notable difference to 2D animations is that the 2D animations all the movement takes place on an x and y-axis which gives it a flat appearance. Whereas in 3D there is a third z-axis, that allows for the result to be rotated and viewed from a number of different angles. (iNurture, 2016)[viii]

IV. Motion Graphics

This is a visual effect technique that is often used within the advertising industry or for multimedia projects. Quite simply it is moving graphical elements such as text or logos around the screen through the use of software. (New York Film Academy, 2017)[ix]

V. Stop Motion

Stop Motion is similar to Cel Animation however instead of combining drawings it combines objects such as clay models or puppets that are manipulated for each different frame so that when images of them are combined it creates the movement motion for the watcher. Just like Cel Animation this is incredibly labour intensive and time consuming. (New York Film Academy, 2017)[x]

The animation I am making most broadly aligns to a Motion Graphic.

2.1.2 Why learn through animation?

Richard K. Lowe a professor of Learning Technologies at Curtin University describes two main reasons to use animations as tools for education: affective and cognitive. (Lowe, 2004)[xi]

The affective function is to gain the users attention and keep them in engaged in the material, through this it sustains their motivation for learning. If an animation is affectively orientated it is often shown to be humorous, spectacular or bizarre and these features can have little relation to helping the user understand the information itself.

The cognitive function is where animations are used to support the user's cognitive processes that allow them to understand the information itself.

There are many proposed benefits of animations for the use of learning such as providing both pictorial and verbal information, the graphics attract attention and often save explaining content in words that can be shown instead. Tversky, Morrison and Betrancourt, 2002)[xii]. Furthermore, as discussed above through the affective function it keeps the user motivated and interested in the subject matter for longer. However, despite these proposed benefits research shows it is still disputed whether animations improve learning compared to static material.

From (Tversky, Morrison and Betrancourt, 2002)[xiii] work they state there isn't clear evidence that it improves learning due to many experiments not having an accurate equivalent material to compare it to. They discuss several examples of previous experiments that conclude animation do enhance users learning however Tversky, Morrison and Betrancourt state on closer examination these studies are again not proof of animation improving learning. This is because they contain more information than the static images and that is often the reason for enhanced leaning, if the static images or content contained equal information this would then be a reliable form to ascertain if the animation itself enhances the users learning.

It is clear from this paper they attribute improved learning to either the interactivity or prediction within the animation that is a known feature to enhance learning not the animation itself. Alternatively, it is due to the animation itself containing more information than the static content given to the user. Although it may not be the animation itself specifically improving the users learning, I think it is clear the animation still helps to facilitate the enhanced learning of the material whether that be by inadvertently providing more information in a fun way or through other learning elements such as being interactive.

A key point from this article is that animation interactivity is the key element to enhancing its benefits and beating any negatives elements. This includes allowing the user to control the speed of the animation and allowing them to play, pause, review, zoom in or out and to change the orientation. This will allow for a successful animation to be made that doesn't cause users to have to sit through subject matter they already know. Furthermore, it will result in an animation that depicts either high level steps or a series of microsteps that animations are well-suited to portray. (Tversky, Morrison and Betrancourt, 2002)[xiv]. This is further supported by (Malamed, 2016)[xv] who has identified the key problems with educational animations and how to resolve them, the first being pacing. Shown in figure 1 beneath. I will use these to help me in the design stage of my animation to enable my animation to be as beneficial to the user as possible.

Problem	Fix
Pacing. Researchers say that a key problem with the animation format is information overload. Most instructional animations are not paced for the limited capacity of working memory. During an animation, learners must quickly select the relevant information and hold that information in memory to integrate it with what comes next. This creates a high cognitive load that may hinder the resources available for learning.	Provide controls so the learner can slow down the animation to a comfortable pace. Allow users to rewind the animation.
Split Attention. When an animated sequence requires reading text and watching the animation, it splits the attention of the viewer. Because the viewer cannot attend to both reading and watching movement at the same time, neither channel is attended to properly.	Use voiceover in sync with the animation rather than written text. Place labels next to the objects or process that they represent so attention will not be split.
Difficulties for Novices. Because many animations require the capacity for high cognitive processing, learners who are not familiar with a subject can have a more difficult time comprehending the material.	People with expert knowledge usually know where to focus their attention on task-relevant information. Novices are not as quick to determine where to focus. Complex animations, therefore, tend to be more beneficial to those with greater subject knowledge and experience. Novices may benefit more from static graphics than from animations.
Fewer Graphic Devices. Certain "visuospatial" techniques of static graphics, such as cross-sections and exaggeration of important features, enhance learning and reduce information overload. There are no corresponding temporal approaches to these techniques.	If these types of graphical devices are the best choice, then replace the animation with a series of static graphics that depict the key phases of the animation.
Not Sure Where to Look. It can be hard for learners to quickly determine which parts of an animation are most relevant and which are not. In fact, some of the more dazzling elements may not be the most important but will attract the most attention.	Use visual cueing devices in animations to point out where learners should place their attention. There is some evidence that a spotlight cue (where less important areas are shaded) is effective. In another experiment, arrows were not as effective as spreading color cues overlaid on salient parts of the animation (kind of like ribbons). The color should spread synchronously with important events.
illusion of Learning. Some researchers report that students may enjoy watching animations over static graphics. This positive affect creates the illusion that the learner has acquired more knowledge or skill than assessment results show.	Use appropriate methods to determine if learning is taking place. Don't rely on self-reporting alone.

Figure 1 - Problems with animations and how to fix them (Malamed, 2016)[x]

It is clear from the (Tversky, Morrison and Betrancourt, 2002)[xvi] that proof of animation enhancing learning is widely disputed and not a small feat to be able to compare. Therefore, after uncovering this research and reading different research papers on the matter it has demonstrated to myself that being able to prove that animations are a better form of learning than static sources is going to be out of reach within the timeframe of this project.

It was mentioned in my initial plan to prove this (as it was first thought it could be a subsidiary element to this project) but in light of this research and, from speaking with my supervisor, I will not be conducting comparisons to other information material within this project. The core aims and objectives still remain, this being to produce an educational tool on security concepts that improve the students understanding through researched learning techniques. This will work towards filling a knowledge gap discussed in the introduction and providing more online resources for learning especially since the world has seen a drastic move to online learning due to the Covid-19 Pandemic.

From the research I have undertaken I have identified several areas I will be including in my project. This includes the ability of a user to control the speed as well as play and pause. Similarly, as animations with interaction and prediction could be the attributed reasons for enchanted learning, I aim to make these a key feature of all animations I create. This leads me onto the next area I researched which explores the interaction in learning as well as visual learning compared to verbal/written, in order to further identify features that will be beneficial for my animation to include. Using the insights from my research I aim to create the best likelihood of the animation improving student's learning.

2.1.3 Interactive learning

By definition interactive means

"allowing a two-way flow of information between a computer and a computer-user; responding to a user's input." (Oxford Languages, 2021)[xvii]

Having learning be interactive brings a variety of benefits such as improving people's retention of information, as people remember 70-80% more of what they visually see as appose to what they read. Additionally, it allows for users to have more flexible access to learning materials and learn at their own pace and in their own time. Lastly, if the interactive material is designed in a consistent manner, then it reduces any variation between content delivered by different instructors, that can hamper students learning. (Ibrahim and Al-Shara, 2007)[xviii]

By allowing students to learn at their own pace, make mistakes and correct themselves without facing any fear of asking something and being wrong it can foster a great environment for learning.

The clear conclusion from (Ibrahim and Al-Shara, 2007)[xix] is that having interactive elements to an individual's learning dramatically improves their retention of the information and that this has been undervalued as a learning tool. It is apparent it should be used as an enhancement to learn and not an altogether replacement of other learning methods. This research has made clear the benefits of having interactive elements within my animation, therefore this will be a key factor when designing my animation.

2.1.4 Colour psychology

I undertook research into the use of colour within learning as I know the use of colour is very important within human computer interaction. From (shiftelearning, 2021)[xx] it is said 80% of information viewed on the internet is obtained through sight and alternative studies have found that users are extremely sensitive to visual cues when learning. Therefore, this is something I will make sure I am applying when designing the visual look of my animation to ensure I am enhancing the user's knowledge retention and understanding. Figure 2 shows a graphic highlighting the 6 main features to incorporate into an eLearning design tool, these take both physiological and psychological effects into account. I will use these 6 features when designing my animation and through this I hope to gain benefits such as stated in (shiftelearning, 2021)[xxi] of colour improving learning from 55% to 78% and improving comprehension by up to 73%.

Figure 2 Shift Disruptive elearning (shiftelearning, 2021)[xv]

2.1.5 Retrieval based learning

Retrieval based learning has been a learning technique since I can actively remember from my own education as it was often encouraged to test yourself and repeatedly looking at text covering it and then trying to remember what was there. This act being encouraged in education is mostly due to the fact actions of repeatedly retrieving knowledge does have a great impact on learning due to it enhancing long-term retention (Karpicke and Bauernschmidt, 2011)[xxii].

Since Retrieval based learning is a well-used and proven effective learning technique, I think it is important to utilise within my animation. Possible options to implement as an animation form of retrieval-based learning are flashcards, practice problems and writing prompts. They all are methods of retrieval practice as it causes the user to have to recall information from their memory without looking at it which causes a challenge and that act is what improves long-term learning over short-term (What is retrieval practice, 2019)[xxiii]. It is also beneficial as it allows for the user to identify gaps in their learning and subject areas where they may need to go over.

2.1.6 Other educational animations out there

I have investigated existing educational animations that are available and will go through each one below. For the topic of RSA I did not find an interactive animation, which is not to say one doesn't exist, but it is not readily available.

The first animation I found is a 4-minute-long video showing the animation of asymmetric encryption with a voice speaking over the top shown in figure 3. (Simply Explained, 2017)[xxiv]

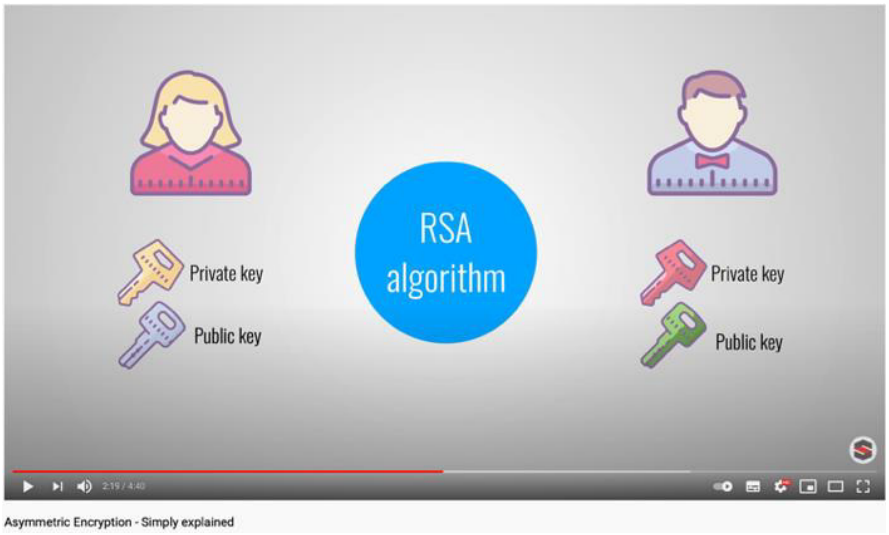


Figure 3 Existing animation on Public-Key Cryptography (Simply Explained, 2017)[xxiv]

There is a period of one whole minute where the voice over is just speaking and no movement in the animation is taking place. This requires the user to have to be intently listening similar to being in a classroom and have to click back if you missed something. It doesn't allow the user to take information in at their pace. This is different to the animation I intend to make. I will not have large voiceovers; the information will be shown to the user to take in at their own pace. Additionally, the user will be able to use features like a drag bar to rewind the animation. Whereas in a video you have to skip back to re-watch something. This animation does use very clear images for the "Alice" and "Bob" as well as the keys which I think is very useful. My animation will have similar useful imagery. Finally, as this is a video animation there are no interactive elements, which is the significant difference to my animation.

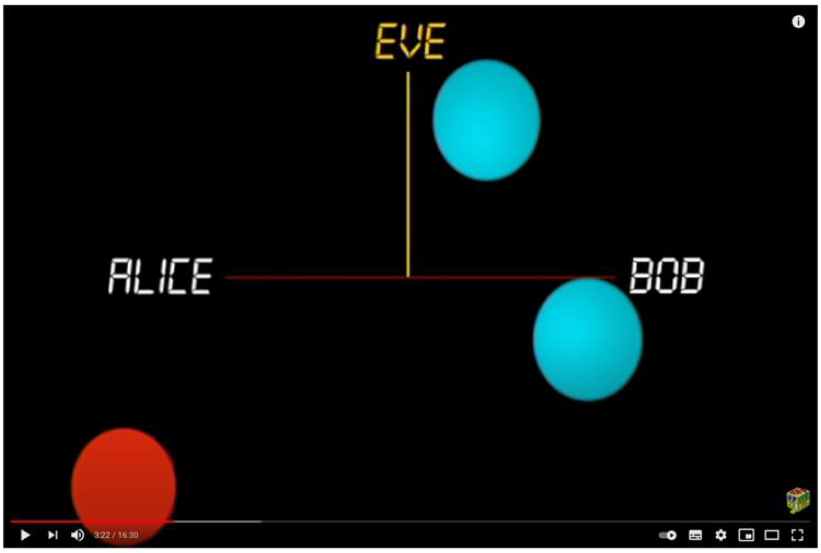


Figure 4 - Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv]

Another animation I found of RSA is a 16 minute and 30 second animation video which is incredibly long (Art of the Problem, 2012)[xxv]. Figure 4 shows the styling of this animation. Figure 4 according to the speaker is Alice sending her public key to Bob but this is not visually very obvious when the user pauses the video as circular blocks of colour are being used to represent the transfer of both keys and the message.

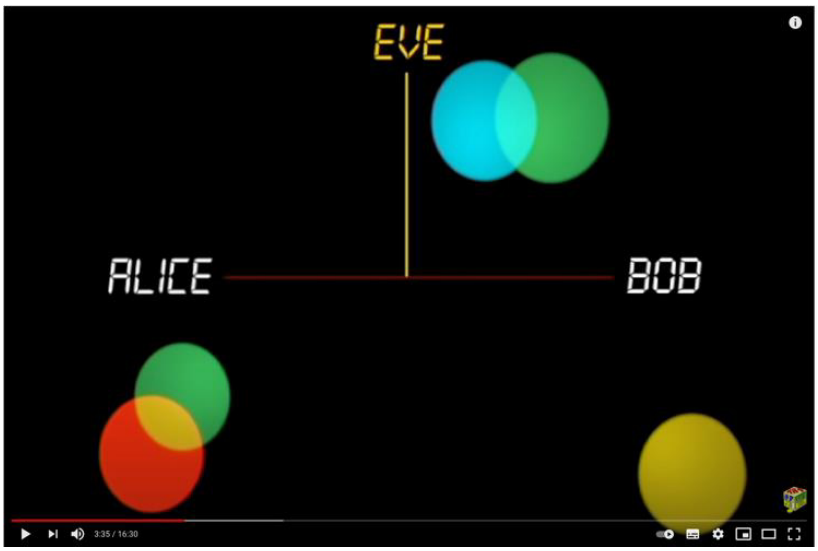


Figure 5 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv]

Figure 5 is showing the animation using an analogy of mixing colours to show the user how a message combines with the public key. This is represented by the blue circle being Alice's public key, which she sends to bob, bob then combines the blue circle with his "secret yellow" as said in the video and sends the resulting green circle to Alice, as shown in figure 5. When Alice then adds her "private colour" as said in the video which is the red circle to "taking the colour off" and reveal yellow secret colour. The animation at the same time shows Eve's involvement. I found this to be a lot of information to take in at what was a very quick speed. Trying to understand what was happening between Alice and Bob, whilst simultaneously seeing Eve the attackers involvement was very difficult, even with knowledge of how RSA works I found it hard to follow. Especially as the analogy of the colours made it hard to understand what the real-world implications were and the correct terminology wording such as "secret yellow" was used for the message that was being sent.

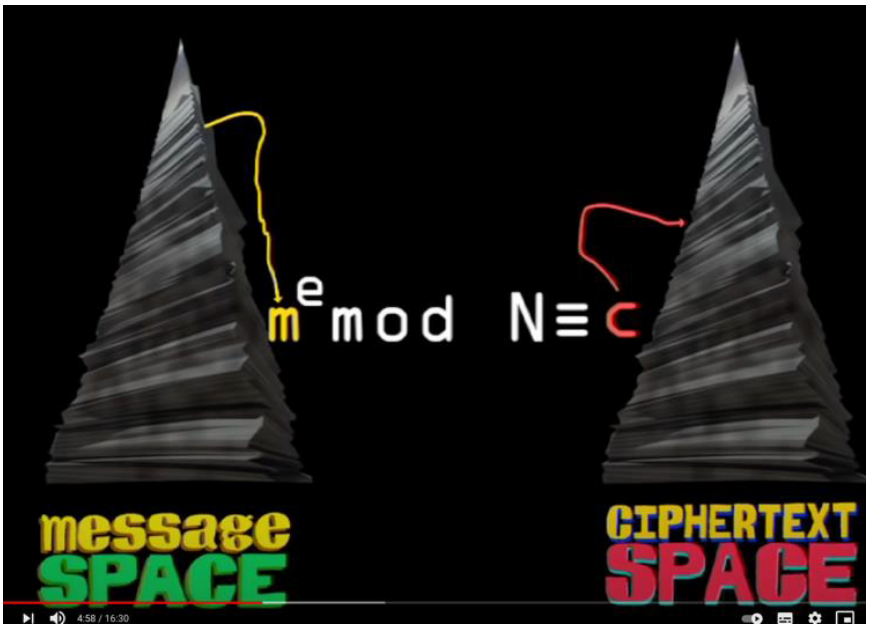


Figure 6 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv]

For my animation I will ensure I am delivering information in a slower and more understandable pace. Additionally, I will deliver concepts individually, for example I will first show the user the interactions between Alice and Bob before then including Eve the attacker. I will allow the user to digest information in smaller segments and then move on to the next animation to gradually progress their understanding. Allowing the user to go back to each area of information as they wish. Furthermore, I will not be using an analogy for animation as I found it more confusing than helpful.

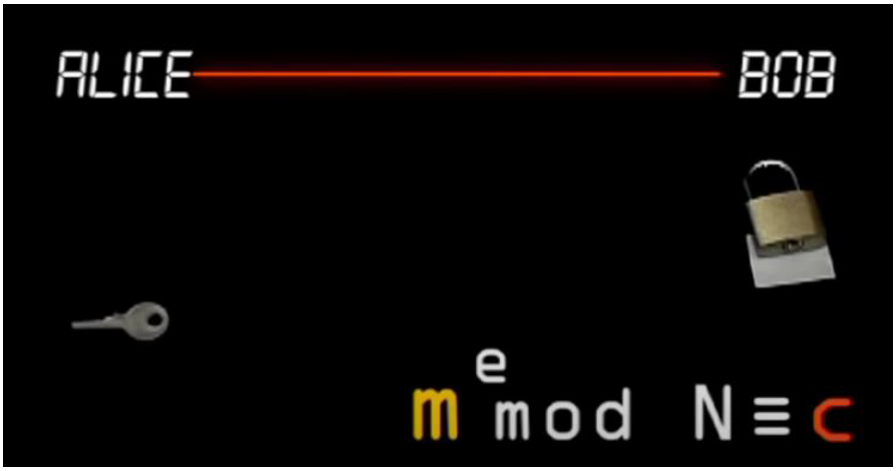


Figure 7 Asymmetric Encryption Animation Example (Art of the Problem, 2012) [xxv]

The animation goes on to explain the use of modulo as part of RSA. However, again this was delivered very quickly and not clear on exactly what was happening. Figure 6 and 7 below show a brief view of how the animation explained this. Figure 6 shows the message space vs the ciphertext which I aim to show through the use of colour in a more definitive way, perhaps through dividing the screen. Figure 7 shows the mathematics of the message taking place between Alice and Bob. This shows the elements of the equation flying around the screen again at a quick pace that is difficult to understand, especially in terms of how each element is involved in the encryption and decryption of a message.

Another source I have looked into (F. Learning Studio, 2020)[xxvi] which gives 5 good examples of animations, with very pleasing colour schemes, storytelling and narrative elements to help the user follow at a good pace. They were much easier to digest the information as were in smaller segments. This is something I aim to utilise by having several smaller animations, that the user can progress through. This will also allow the user to find each part of information separately and not face one large video like the earlier examples I found.
From this article it was said that

"Colorful character design, storytelling elements of videos can brighten the tone of the virtual classroom and grab the learners' attention." - (F. Learning Studio, 2020)[xxvii]

This is something I agree with and aim to incorporate into my animation.

All of the animations I have discussed so far are not interactive. I have found an interactive learning tool (not an animation) which is on machine learning that I think had some interesting features, figure 9 (R2d3.us, 2019)[xxviii]. It allows the user to scroll through the learning tool and as they do the text on the left changes as well as the graphics on the right-hand size gradually fading into more complex representations or new graphics completely, as shown in figure 10 and 8.

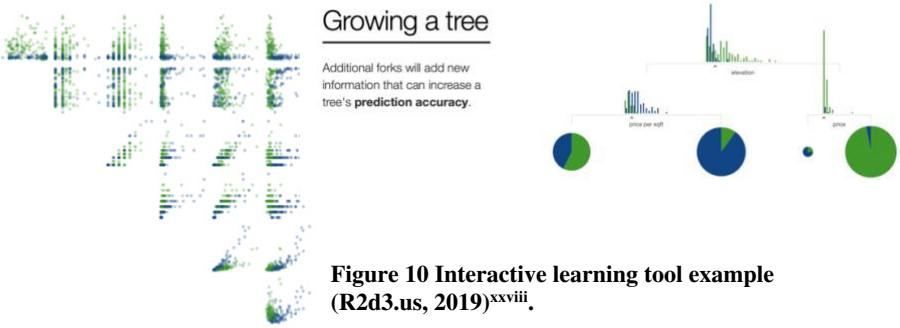


Figure 10 Interactive learning tool example (R2d3.us, 2019)[xxviii].

Figure 9 Interactive learning tool example (R2d3.us, 2019)[xxviii].

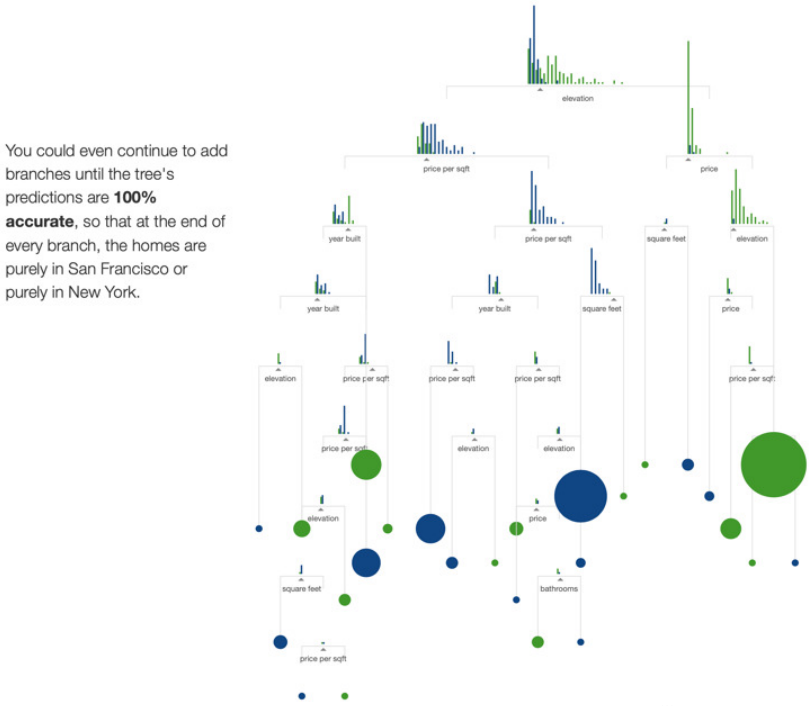


Figure 8 Interactive learning tool example (R2d3.us, 2019)[xxviii].

This learning tool demonstrates a important point I want to incorporate into my animation which is key for helping to learn as discussed earlier and that is the ability for the user to interact with the learning material. Therefore, on areas where I need to deliver a lot of text the feature of information appearing as the user scrolls for example is very beneficial and I intend to use a similar feature in my animation to deliver text content.

2.2 Background material

My project is about animating security concepts and as discussed in my initial plan I was going to spend some time researching and deciding on which security concepts to animate. Firstly, I looked at what computer security is. The NIST Computer Security Handbook [NIST95] defines computer security as the following:

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)." -
(Guttman and Roback, 1995)[xxix]

The three key objectives hoped to achieve from this term is; confidentiality, integrity and availability.

From this I found there to be two main areas which were cryptographic algorithms and protocols. These are further broken down into the following four categories: (Stallings, 2017)[xxx]

I. Symmetric encryption
II. Asymmetric encryption
III. Data integrity algorithms
IV. Authentication protocols

From this I chose to focus on Asymmetric encryption and the next section details background information on this as well as the route I chose to focus on.

2.2.1 Public-Key Cryptography and RSA

Public-key Cryptography also known as asymmetric Cryptography is a significant development from its predecessors which mainly consisted of using substitution and permutation to encrypt messages. Public-key cryptography uses mathematical functions for its core functionality, instead of substitution and permutation. Additionally, in comparison to symmetric Cryptography that only uses one key, public-key uses two keys. Which are known as a public-key and a private-key, the use of two keys brings benefits such as confidentiality, key distribution and authentication. Figure 11 shows some key terms related to Asymmetric Encryption (Stallings, 2017)[xxxi].

Asymmetric Keys
Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Public Key Certificate
A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key.

Public Key (Asymmetric) Cryptographic Algorithm
A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Public Key Infrastructure (PKI)
A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Figure 11 Terminology Related to Asymmetric Encryption (Stallings, 2017)[xxxi] page 285

Public-Key Cryptography combats two main problems with symmetric Cryptography, which are the need for the two communicators needing to share a key which has been distributed to them in a certain way and secondly the need for a key distribution centre.

Figure 12 details the encryption and decryption process of Public-Key Cryptography. That I intend to teach within my animation.

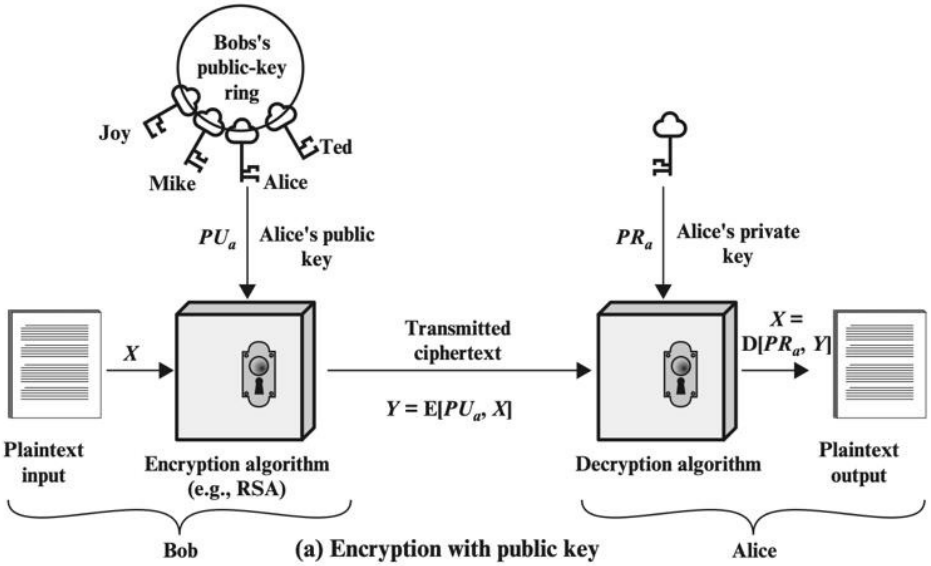


Figure 12 Encryption Process (Stallings, 2017)[xxxi] page 287

Figure 13 details the decryption process that again will be taught within my animation.

- **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

The essential steps are the following.

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private. As Figure 9.1a suggests, each user maintains a collection of public keys obtained from others.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

Figure 13 Decryption Process Stallings, 2017)[xxxi] page 288

There are three rough categories that the applications of public-key cryptosystems can be placed into (Stallings, 2017)[xxxii]:

I. **Encryption/decryption of messages**
II. **Digital signatures** where a user uses their private key to "sign" a message as a way of authenticating who sent the message.
III. **Key exchange** used to give a session key (a secret key for symmetric encryption) to another user.

Different algorithms are used for the above applications and figure 14 shows which algorithms are applicable to each application.

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes
DSS	No	Yes	No

Figure 14 Applications of Public-Key Cryptosystems (Stallings, 2017)[xxxi] page 292

I have chosen in my animation to implement RSA and Diffie-Hellman specifically as between them It can be applied to all three applications which will be great to demonstrate in my animation, the three different applications and using more than one algorithm. The next section explains how RSA and Diffie-Hellman works.

2.2.2 RSA

Figure 15 shows the process of key generation by Alice and then how Bob encrypts a message using Alice's Public Key to convert into a Ciphertext that is safe to send across the internet to Alice. It can also be seen from figure 15 how Alice can then decrypt this message. This process is again something I wish to give the users an understanding of after finishing watching my animation. Figure 16 gives a numerical example of this process which I intend to show in my animation.

Key Generation by Alice	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 15 Key Generation, Encryption and Decryption (Stallings, 2017)[xxxi] page 297

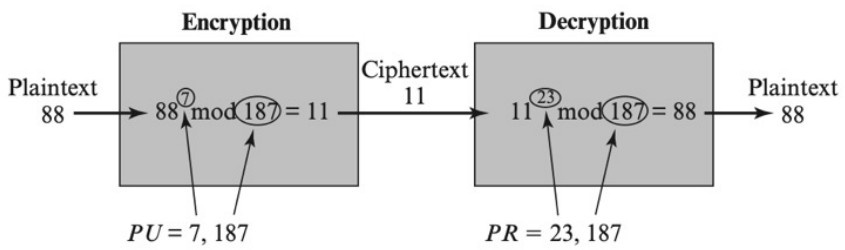


Figure 16 Encryption and Decryption (Stallings, 2017)[xxxi] page 297

2.2.3 Diffie-Hellman

Figure 17 shows the process involved in the key exchange using Diffie-Hellman. This process will be depicted within my animation.

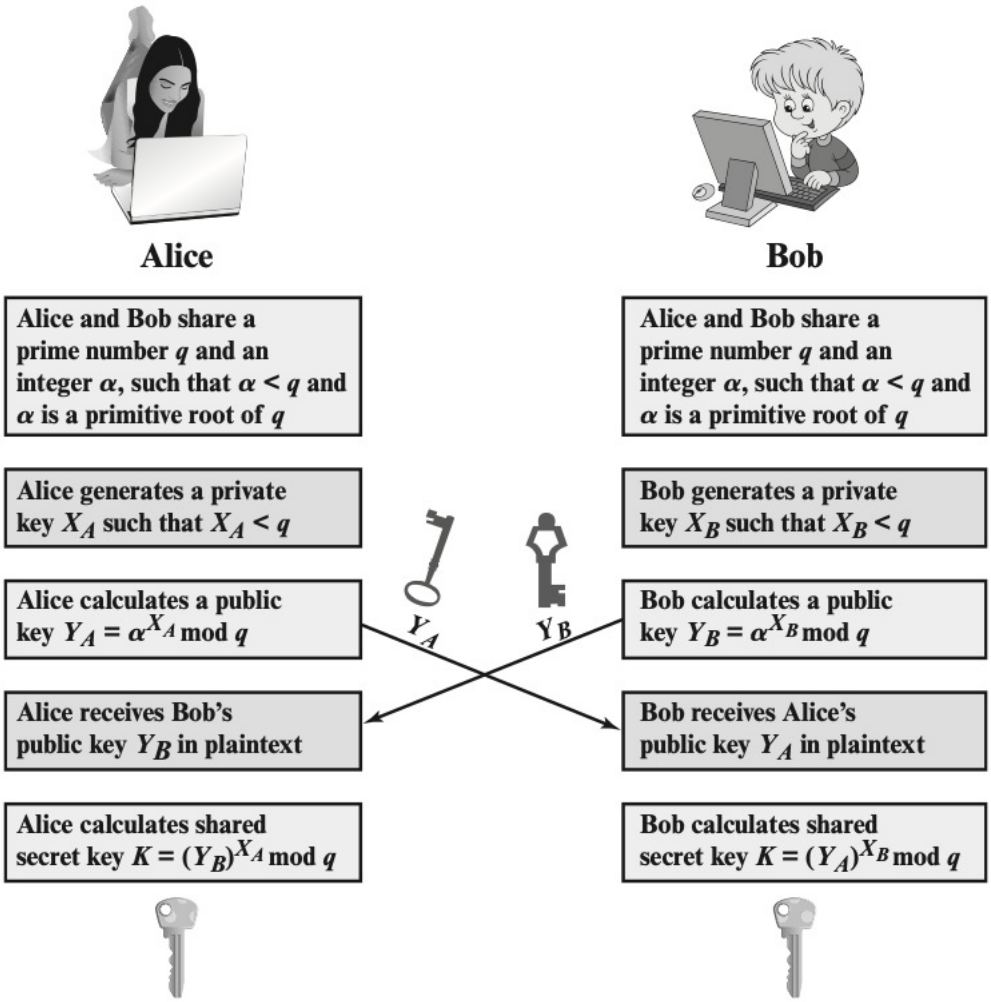


Figure 17 Diffie-Hellman (Stallings, 2017)[xxxi] page 315

2.3 Human Computer Interaction

Human-computer interaction (HCI) is the field of study that specialises in the design of computer technology and, more specifically, the interaction between the users of computers (humans) and computers. HCI was originally focussed on computers but over time it has digressed to cover most forms of design within technology. - (Interaction Design Foundation, 2014)[xxxiii]

HCI allows designers to endeavour to create a user-friendly interface and interactions between the user of the system and the system itself. This is why I will be using Nielsen's Ten Heuristic Principles to aid in my design process (Tutorialspoint, 2019)[xxxiv]. Additionally, in order to try and meet these principles in the first place in the design stage I will discuss user personas and user journeys to enable my project to meet these heuristics.

Nielsen's Ten Heuristic Principles: (Nielsen, n.d.)[xxxv]

1. Visibility of system status.
2. Match between system and real world.
3. User control and freedom.
4. Consistency and standards.
5. Error prevention.
6. Recognition rather than Recall.
7. Flexibility and efficiency of use.
8. Aesthetic and minimalist design.
9. Help, diagnosis and recovery from errors.
10. Documentation and Help

I have also investigated eLearning principles that I intend to use in the design process to shape my animation and to evaluate my animation against. The principles I have chosen is Richard E. Mayer's 12 principles from his Multimedia Learning book (Mayer, 2020)[xxxvi] which are as follows:

1. Coherence Principle
2. Signalling Principle
3. Redundancy Principle
4. Spatial Contiguity Principle
5. Temporal Contiguity Principle
6. Segmenting Principle
7. Pre-training Principle
8. Modality Principle
9. Multimedia Principle
10. Personalisation Principle
11. Voice Principle
12. Image Principle

3. Specification and Design

This section details the specification and planned design of the interactive animation that I will be making for this project. The following items can be found within this section:

3.1. User Personas will highlight the expected user and target audience of this tool.

3.2. MoSCoW Requirements (Must have, Should have, Could have, Wont have time for). This will enable key features to be implemented within the allotted timeline and, if these are met before the allotted development phase, then the desirable requirements will be implemented.

3.3. Overview of each planned animation with a User Interface Design to give a conceptual view of how the interface will look.

3.4. User Journey to show the start to end process the user can take.

3.5. Use Cases to show the main interaction that will take place between the tool and the user, such as using each animation and navigation around the tool.

3.6. Risk Assessment where I have carried out a thorough risk analysis and identified and detailed these in this section. This also shows how to mitigate against these risks in the case of them taking place.

3. 1 User Persona

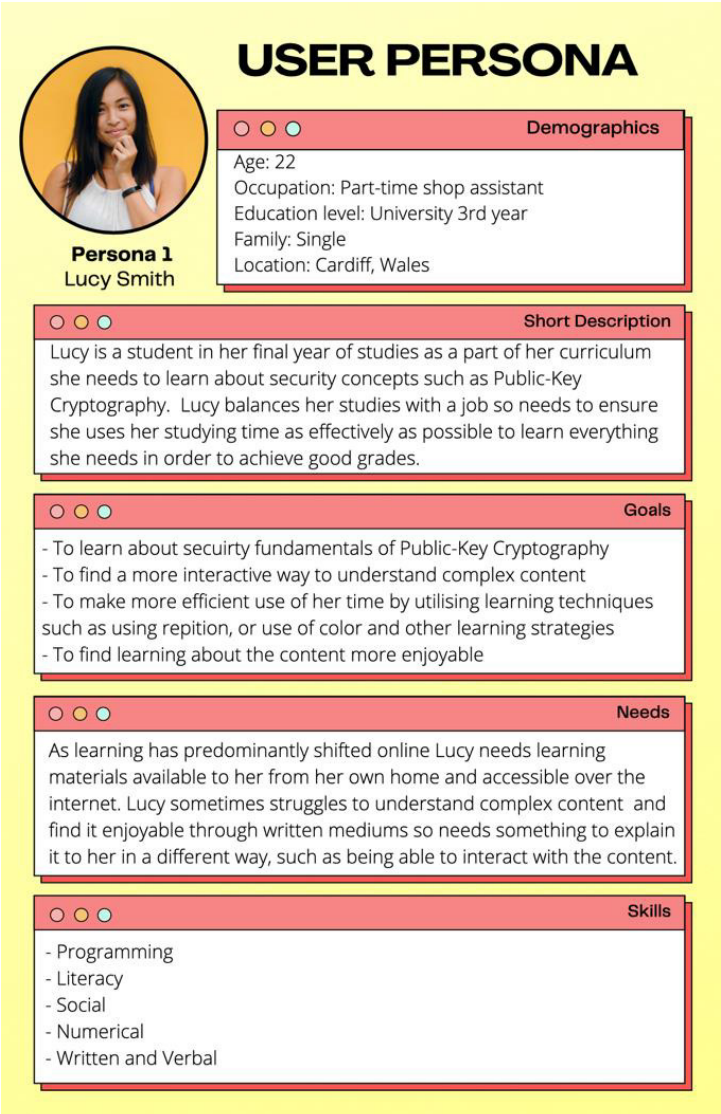


Figure 18 User Persona

3.2 Requirements

In order to manage the workload in this project I have decided to use the MoSCoW prioritisation technique that is commonly used to manage and understand priorities within a project (Agile Business Consortium, 2019)[xxxvii]

3.2.1 Must have Requirements

These are the requirements that the project will guarantee to achieve.

Requirement 1: There must be a working homepage
This is to facilitate a way for the user to choose which topic to view in their own preference order. Additionally, this is to allow several smaller topics to be in more manageable sections for the user to view and return to, unlike some animations I discussed in the earlier sections that were one lengthy animation. By having smaller more manageable sections of information for the user I hope to create greater enjoyment and motivation.
Requirement 2: There must be at least one animation dedicated to each of the three applications of Public-Key Cryptography (Message Exchange, Digital Signatures and Key Exchange
In my research I have identified that there are three main applications of Public-Key Cryptography, therefore I think it is essential to cover all three to provide a full coverage of Public-Key Crypto-systems.
Requirement 3: The tool must have a consistent colour scheme and layout
This is essential to ensure the user experience is enjoyable and the user is able to navigate the system without confusion.
Requirement 4: The tool must have interactive elements for the user on every animation
As part of this project a core element is to create "interactive" animations. Therefore, to ensure I fulfil this each animation must have at least one interaction with the user. The nature of the interactive elements will be based on the research conducted earlier.
Requirement 4: The tool must run on Windows and Mac operating systems.
This is to ensure it is accessible for users with different operating systems. I myself, as a Mac OS user, have experienced in my final years of studies not being able to access some online learning tools that are only compatible with Windows OS. This can lead to unfairness amongst student provided learning tools.

3.2.2 Should have Requirements

These requirements are very important to achieve but are not vital for a successful outcome.

Requirement 6: There should be an interactive flash card feature
As human recall and repetition are such useful learning features this tool should utilise this and create a flash cards section that allows users to turn over cards to show and hide answers enabling users to test their learning.
Requirement 7: There should be an animation showing a man in the middle attack on Diffie-Hellman Key Exchange
As a key area in learning about cryptosystems is the security of them, I believe it is necessary that this tool should have a minimum of one animation showing an attack. As man-in-the middle attack is very prominent in textbooks and teachings of security I have decided this should be shown in my animation.
Requirement 8: There should be an animation showing the mathematics behind a message exchange with RSA
A key part in learning about the three applications of Public-Key Cryptography is knowing how in practice its implemented. Therefore, this animation should show this through showing key generation, encryption and decryption.
Requirement 9: There should be an animation showing the mathematics behind Digital Signatures with RSA

A key part in learning about the three applications of Public-Key Cryptography is knowing how in practice its implemented. Therefore, this animation should show this through showing key generation, signature creation authentication of signatures.
Requirement 10: The system should not have any error pages generated
For usability it is important that no navigation buttons should cause the user to arrive at an error 404 page.
Requirement 11: The system should base timings of reading animated text on average user reading times.
This is to ensure good usability for the user. Therefore, calculations will be carried out to justify the time given to text shown.

3.2.3 Could have Requirements:

These requirements are desirable and would improve the tool made, however they will have a small impact if not completed.

Requirement 12: The system could have colour coding for different variables.
To enhance users understanding keys and description of each could be colour coded to help the users follow what is being shown.
Requirement 13: The system could have an animation showing the mathematics behind a key exchange and man in the middle attack
If there is time the mathematics of Diffie-Hellman could be shown, however this is a could be requirement because of how many animations are already designated as must or should and therefore of greater priority.

3.2.4 Won't have time Requirements:

These requirements have been identified as beneficial to the project, however there is not time to achieve them within the available timescale for the project so will not be included at this stage. They could be considered for future work.

Requirement 14: To have a quiz feature at the end to test the users.
This would be desirable to give the user feedback on their understanding and act as a further opportunity to recall what they have learnt as retrieval and recall are a useful learning aid as discussed in the research.
Requirement 15: To have drag and drop interactive elements for the user to use
Whilst researching available interactive animations I have found that some have the ability for the user to select an object from a fixed location, drag and then drop it to somewhere on the screen to either test if they placed it near the correct answer for example or just to enable them to see the effect of moving it. I found this to be very enjoyable and fun to use, especially for the purposes of learning. However, upon investigation of the code in such examples it was extremely complex, and I am starting with no knowledge on coding an animation and such features so there is not time within this project to create such a complex advanced features.

Acceptance Criteria for each requirement will be assessed as a YES or NO.

3.3 System Structure

As seen in figure 19 my tool will be built as a web based front end that consists of a HTML, CSS and JavaScript file utilising anime.js library to construct the page presented to the user and create the animations within each page.

For my tool there is no back-end structure being implemented.

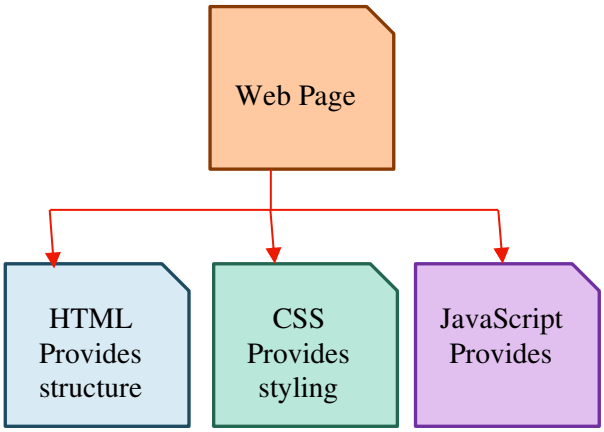


Figure 19 File Structure

Figure 20 shows a Site Map of my website I will create that will host the animations on.

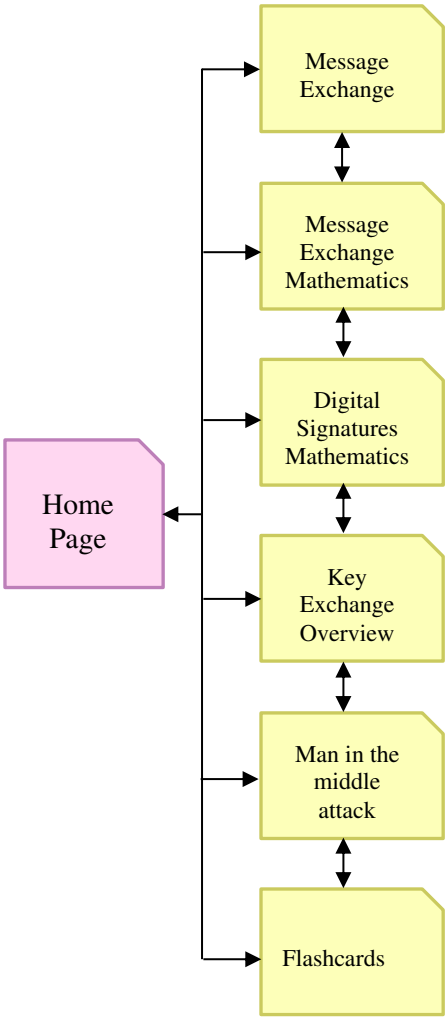


Figure 20 Site Map

3.4 Design Decision of JavaScript modules

I have selected to use anime.js JavaScript library to implement my animation. There were many available options, I chose anime.js due it being highly recommended on review sites ranked first and also due to its 39 thousand stars on GitHub, which is significantly more than other options available such as Velocity.js. (Priya, 2020)[xxxviii]. Additionally, because it is referred to as lightweight, has a single API and it can be used to animate HTML, CSS, JS, SVG and DOM attributes which I believe will be fully sufficient for everything I wish to animate (Priya, 2020)[xxxix].

From investigating the language further, the ability to use staggering will be very beneficial as I will be able to overlap movement which will be necessary with showing how public-key cryptography works I believe (such as showing a key being applied to a message and a lock appearing at the same time).

Lastly from my research I established having a play, pause and rewind feature was integral in allowing the user to control the pace of the information presented to them in order to aid in their learning. This is something I ensured anime.js allowed for before selecting it. It also allows for built-in call-back and control functions that I found whilst reading the documentation that highlights and provides examples on all of anime.js features (animejs.com, n.d.)[xl]. This live reverse and fast forward feature will be a key differentiation in my animation compared to other non-interactive animations.

All of the above is my justification for picking this library and during my decision process I found that the anime documentation and a site called Code pen (CodePen, n.d.)[xli] which provide a multitude of examples which will be my key areas to seek examples and view the capabilities of anime.js when implementing my design. The animation documentation demonstrated the movements possible to achieve. As a complete beginner to creating JavaScript animations this will be a very useful teaching source for my coding such unfamiliar content.

3.5 User Interface Designs

3.5.1 Homepage

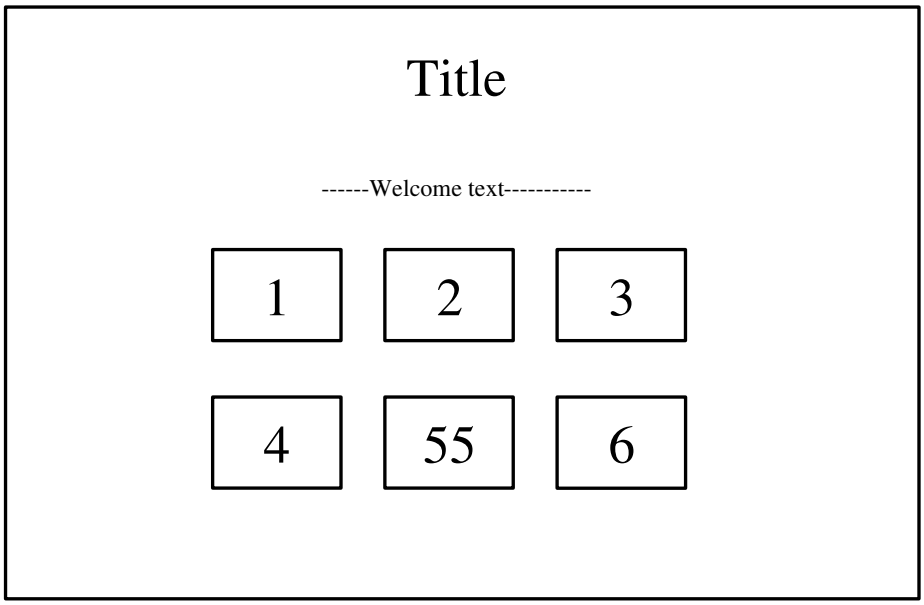


Figure 21 Home Page UI Design

Features and Justification:

1. Title

i. At the top of the page clear and familiar to the user.

2. Introduction text

i. To welcome the user and instruct them they can click the buttons below to progress through each mini topic.

3. Central buttons to take the user to each animation

i. These will be interactive in that when the user hovers they will rotate as a 3D cube to a second face saying, "Click Me".

ii. From my research I based the decision to divide the content I wanted to deliver into smaller segments than other animations on the same subject matter that were very lengthy. Additionally, from my research I learnt how users being able to work at their own pace is better for their learning therefore the segments allow the user to divide up their workload and return to each sub-topic when they wish.

This page enforces HCI Principle 9 of an aesthetic and minimalistic Design that is kept throughout all the UI Designs. It also allows for Principle 3 of User Control and freedom by allowing the user where to start and finish additionally by supporting multiple paths to take with the system.

3.5.2 Overview of Message exchange, Key Exchange and Man in the middle template page

Figure 22 shows the template for creating each overview animation. This will remain the same for all three to ensure consistency and familiarity for the user.

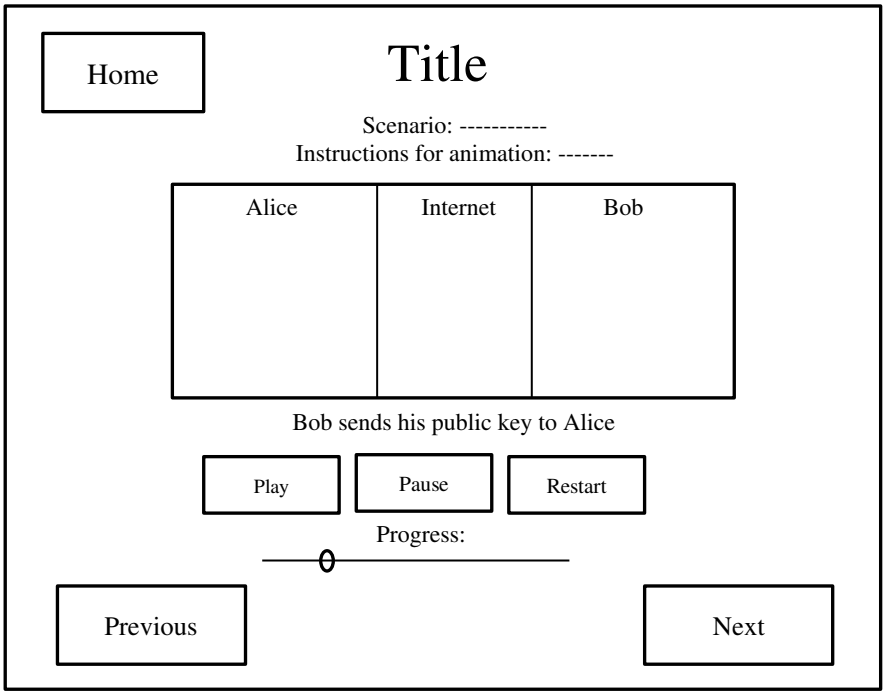


Figure 22 Timeline animation UI Design

Features and Justification:

1. Home Button
   a. In the top left corner familiar to users
2. Text Scenario:
   a. There will be text below the title detailing the scenario of the animation such as "Alice wants to send a message to Bob using Public-Key Cryptography without anyone else being able to read the message, the animation shows you how". This will be followed be brief instructions on the animation such as "use the buttons and progress bar below to play, pause and rewind". This allows for assisting the user in their journey.

3. Central animation box
    a. This box will be where the animation is shown. There will be three divided columns of colour to show the user clearly when items such as keys are just visible to Bob, Alice or anyone over the internet.
    b. Images of the keys, messages and a lock to represent an encrypted message and therefore unable to read will fade in move across the screen and fade out as per the order of Public-Key Cryptosystem.
4. Below the Central Box is text that will fade in and out as a part of the explanation process with the moving elements. The timings of the text being shown to the user will be calculated based on the average user reading 200 words per 60 seconds (Execuread.com, 2012)[xlii].
5. Control Buttons
    a. There will be play, pause, restart buttons as well as a sliding bar at the bottom for the user to be able to at their own pace view the animation. This was highlighted in my research as a key tool in helping users learning which is why I have made it the key interactive feature on this animation. The drag bar will move the animations timeline live as the bar is moved. This is a different approach compared to when watching a video and you drag the bar you cannot see the contents move again until you've selected the new slot on the timeline.
6. Previous and Next Buttons
    a. The buttons will enable the user to progress through the animations as well as return to the previous mini lesson. They are placed on the left and on the right respectively to be in intuitive places.

This page enforces HCI Principle 2 of an Match between system and the real world because it follow what users are familiar with such as the play and pause button and the drag bar provides a good mapping between the task and the system. Additionally, Principle 7 Recognition rather than recall as the design suggests what the user needs to do and there is descriptive links in the buttons. Lastly it enforces Principle 8 Flexibility and efficiency of use because it allows for different user sophistication through play/pause buttons or a drag bar to go quicker. Furthermore, by having both options it supports different methods to reach the same end goal of watching the animation through.

3.5.3 Mathematics Explanation template page

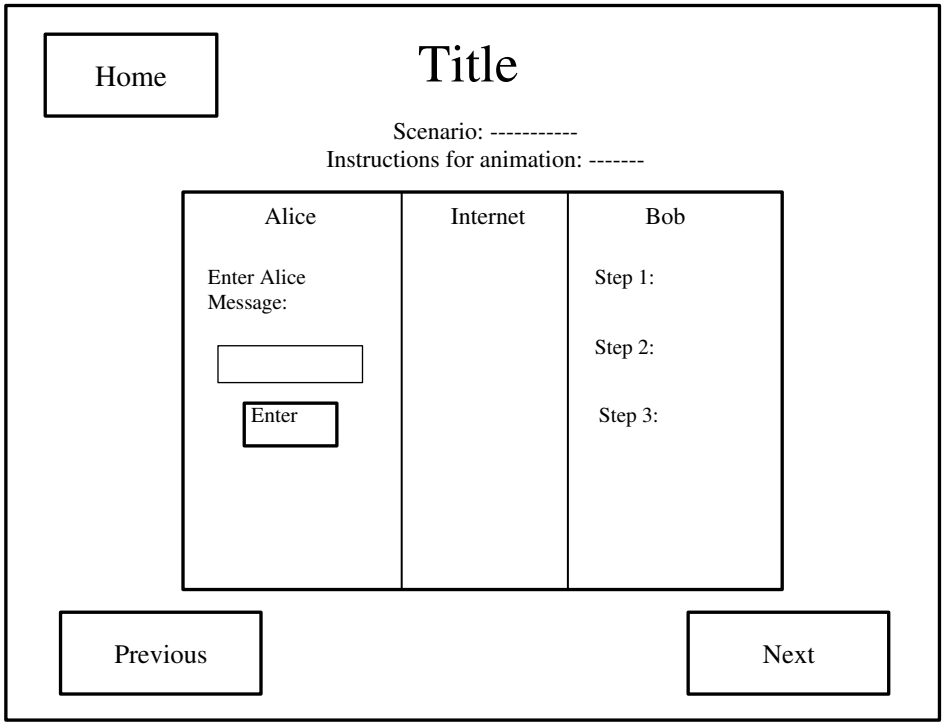


Figure 23 Mathematics UI Design

Features & Justification

1. Home Button
   a. In the top left corner familiar to users
2. Text Scenario:
   a. There will be text below the title detailing the scenario of the animation such as “Alice wants to send a message to Bob using Public-Key Cryptography without anyone else being able to read the message, the animation shows you how”. This will be followed be brief instructions on the animation such as “Click the Steps to progress through the animation”. This allows for assisting the user in their journey.
3. Central animation box
   a. This box will be where the animation is shown. There will be three divided columns of colour to show the user clearly when items such as keys are just visible to Bob, Alice or anyone over the internet.
4. Clickable text
   a. Each step when hovered over will change the mouse cursor to indicate to the user it can be clicked
   b. When selected it will trigger animations such as p and q (two primes used in key generation) to be generated moving the numbers into position, a public key being sent across from Bob to Alice.
5. Input boxes
   a. There will be an entrance box for the user to choose the message that will be encrypted and decrypted. The input box will only accept a number and this number will then be output to them and will cause the correct maths to be presented to them.
   b. There will be validation on the entry boxes to ensure only numbers are entered and as the message x must be less than the value of n-1 this too will be checked in the JavaScript Validation
6. Previous and Next Buttons
   a. The buttons will enable the user to progress through the animations as well as return to the previous mini lesson. They are placed on the left on the right respectively to be in intuitive places.

This page enforces all principles discussed so far for the same reasoning. Additional principles enforced in this animation and previous is principle 10 Help and Documentation. All animations have instructions at the top and a scenario text to help the user understand. Additionally, this animation uses cursor shape changes over each step to further enforce Principle 1 Visibility of System Status. Lastly, this animation enforces principle 5 To help users recover from errors, where a user enters a number greater then n in the input box, text is displayed to them informing them of the correct format of input needed.

3.5.4 Flashcard's page

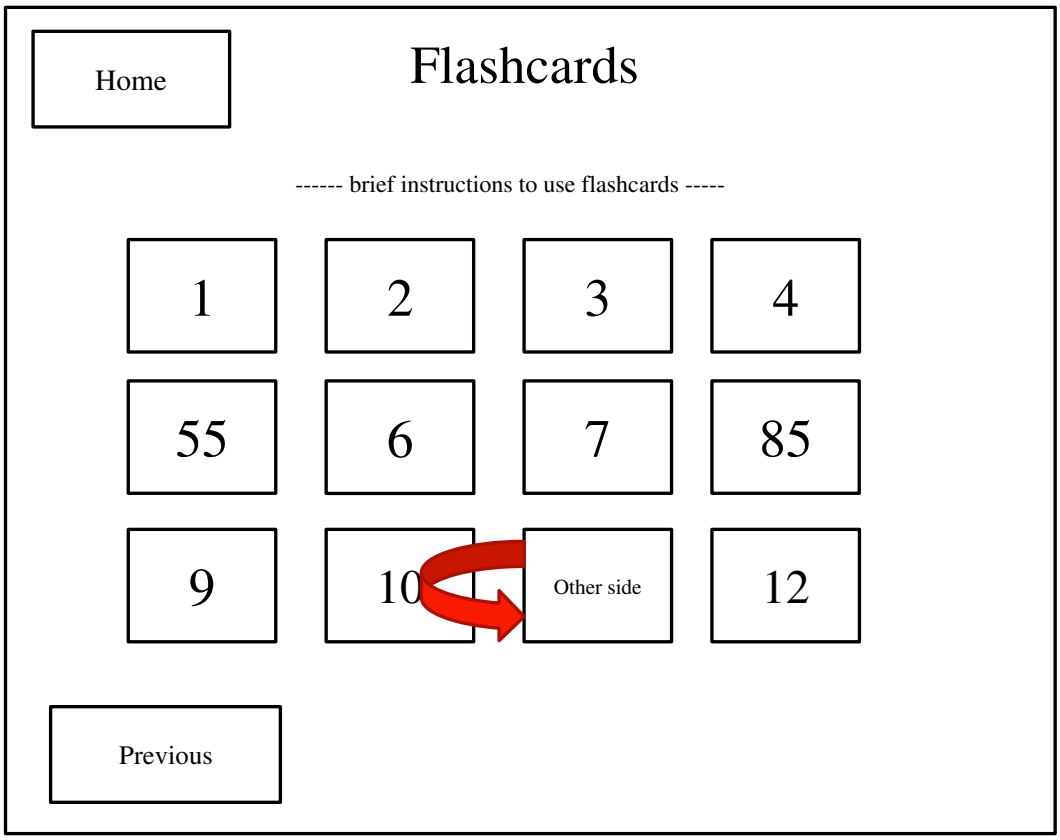


Figure 24 Flash Cards UI Design

Features and Justification:

1. Home Button
   a. In the top left corner familiar to users
2. Text instructions
   a. There will be brief instructions to aid users, informing them to click the animations to test themselves and find out new information on the subject area.
3. Flash cards grid
   a. This will contain a multitude of flash cards that can be used by the user to find out additional information not presented to them in the animation as well as testing them on things they've been shown.
   b. An example is the front card asking for RSA encryption, then when the user clicks a card, it will rotate round looking like a real 3D card moving to reveal the answer of $C=M^e$ mod n. Users would have seen this information in the Mathematics animations, so it provides them for an opportunity of recall which aids in learning as discussed in the research section.
   c. The front and back of the card will be two different colours to utilise the use of colour theory discussed in the research section, allowing the user to make a clear distinction from the prompt/question and the answer
4. Previous Button
   a. This button will enable the user to go to the previous mini lesson.
   b. There is no next button here as this is intended to be the last page. Therefore, the user can either go to the previous or back to the home page to reselect which animation they would like to view.

As the final animation page this one enforces principles previously discussed and all UI designs have been designed with principle 4 in mind of Consistency and Standards. By having consistent words at the top of each, objects such as buttons and central box and operations across all of them.

3.6 Animation Overviews

As shown in the site map there will be six different animations each design plan listed below. The prior section showing user interface designs shows the visual template planned for the six pages. This section details the planned content to be shown in each animation window box, in the order and the movements involved.

3.6.1 Message Exchange Overview

This will be the first animation to be seen and provides an introduction into how public-key cryptography works. Therefore, the information given will be as if there is no prior knowledge.

When the user selects “play” two keys will appear in Bob’s column, one for his public key and one for his private key each in two different colours so the user can differentiate between the two. Bob’s public key will translate across the internet column to arrive at Alice. Where a form of typing will be animated, and a message will then appear. Next, Bob’s public key will move onto the message and a lock will appear to show this is what locks the message. The locked message will then transform to the right back to Bob, where his private key that remained on his side will transfer onto the locked message, removing the lock and showing Bob can now read this message.

3.6.2 Message Exchange Mathematics

The initial design for this animation as seen from the mathematics template is that there will be clickable steps that the user can progress through in their own pace. As mathematics is much harder to define a timeline on. First the user will start by clicking through steps to generate Bob’s keys in his column as they click each step the order shown in 24 will appear with the appropriate numbers moving across the screen into the equations.

After the key is generated, the user can click to send it to Alice, and it will be transferred across the screen. Where the user can enter a number, they wish to encrypt and send to Bob, when they change the number all the equations change to reflect this.

After entering their number, the user then clicks through the steps to encrypt the message, again having each step fade in one after the other with the appropriate numbers fading into the location to demonstrate to the user where each number comes from. For example, once Bob has sent his Public key (n,e) then n and e will move across the screen into the encryption equation. Once the message encryption step is complete the user can click to send the message to Bob in which this will move across their screen to Bob’s column. There the user can click through the decryption steps, to reveal the message they chose for Alice.

3.6.3 Digital Signatures Mathematics

This animation will follow a very similar process to the previous animation discussed. The user can click through the key Generation from Bob’s side of the window. This time they select a message as Bob and enter this number. Once they have done so they click through the steps of generating a signature and then they click to send this message to Alice which navigates across the internet column to Alice. There the user can click through steps to calculate x as Alice and compare to what Bob sent to see if the signature is indeed valid.

3.6.4 Key Exchange

This animation will follow the template shown of the play/pause style animation. Very similarly to the message exchange different colour keys will be used to show how Diffie-Hellman Key Exchange works.

A key will be shown on each side for Alice and Bob representing their private keys they each generate, from this another key will appear on each side showing the public key has been generated each. Then the public keys will both move across the internet column arriving to each other.

Next Alice and Bob's private keys will each respectively move and be added to the public key they've each been sent where a new coloured key will be output, showing the secret key they have both now acquired.

3.6.5 Man-in-the-Middle Attack

This animation will show the same steps/movements as the previous however, when the public keys are moving across the internet an attacker will appear and stop the keys. This attacker will then generate her own keys shown on the screen which she then sends respectively to Alice and Bob as per the attack format. In each column keys will appear showing Alice, Eve and Bob mixing their private key with the keys they have received. The end result will show the colour coded keys being mixed and matching the colour that Eve holds. Four keys will be visible, Alice with her secret key matching one of Eve's, then Eve will have another coloured key showing that will match Bob's. This demonstrates to the user Alice and Bob now share a secret Key with Eve the attacker not Bob.

3.7 User journey

Here I have created a user journey that maps the process that a user such as the individual in my user persona shown earlier would take through the use of my tool.

Scenario: Lucy is taking a Security module as a part of her degree and will be assessed on the content; therefore, she wants to do her best. She has attended her lectures and read some textbooks on the material and wants to improve her understanding of Public-Key Cryptography. She struggles to understand how it works and wants to see how it works practically and be able to interact with the material to see what changes it causes. Lucy finds that viewing information in multiple different formats improves her understanding.

Goals and Expectations: Lucy hopes to be able to understand the movements and transitions involved in Public-Key Cryptography as well as being able to understand and perform the necessary mathematics involved. She expects using this animation to educate herself and allow her to attain good grades in her Security module.

Explore Homepage

- Explores the home page reading the welcome text
- Looks at the different topic options
- Chooses the first Topic 1, hovers over the button which rotates round and then they select it.

Message exchange

- User reads Scenario of the message exchange then selects play
- The animation starts to play, the user watches the animation play.
- Half way through the user selects pause and uses the progress bar to live rewind to rewatch an element they wanted to re watch.
- The user finishes watching the animation, undestands the overview of Public-Key Cryptography and is happy to progress to the next topic

Message Exchange Maths

- User Reads the Scenario
- User selects through the steps by clicking each piece of text and then types in their chosen message to the entry point
- The user continues watching the animation through clicking at their own pace, to see their message encrypted and decrypted.
- Once the user is happy they progress to the next animation with the next button

Digital Signatures Maths

- User Reads the Scenario
- User selects through the steps by clicking each piece of text and then types in their chosen message to the entry point
- The user continues watching the animation through clicking at their own pace, to see their message used to create the digital signature.
- Once the user is happy they progress to the next animation with the next button

Key Exchange

- User reads Scenario of the key exchange then selects play
- The animation starts to play, the user watches the animation play.
- The user finishes watching the animation and is happy to progress to the next topic by clicking the next button

Man in the Middle attack

- User reads Scenario of the man in the middle attack then selects play
- The animation starts to play, the user watches the animation play.
- The user finishes watching the animation and has now watched all the animations available they select next

Flash Cards

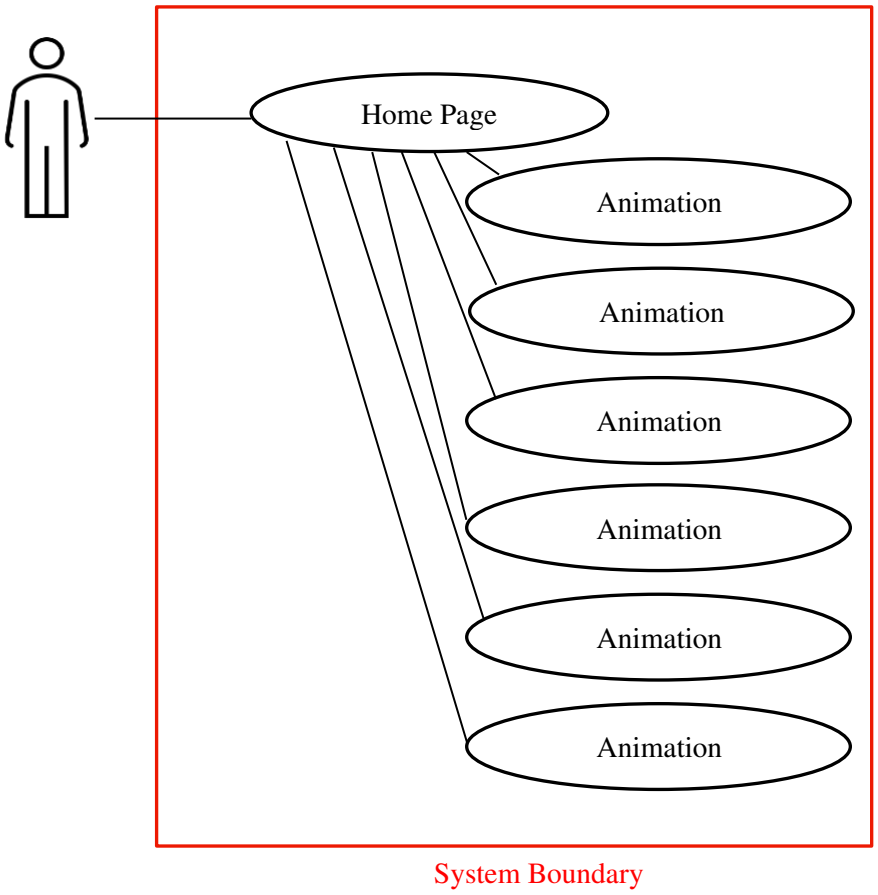
- The user has now viewed all the content and wants to test themselves, the use the flashcards to find out extra information and test them self through recall and repition with the flashcards.
- The user closes the webpage and finishes their study session.

3.8 Use Cases

This section provides a use case to demonstrate how a user will access each animation. Use cases are a useful tool in how a user will navigate around a system. As my animations are mainly movement focussed it would be very complex to do use cases for all movements expected in the animation before beginning implemented. Therefore, I felt it was more appropriate to use the user journey and animation descriptions to provide the details on how each animation will work and provide one use case to demonstrate my awareness of their use in projects.

Use Case Name	Choose Animation
ID	1
Description	The user will be able to decide and choose one of the animations to view from the homepage and navigate to it.
Actors	Student
Pre-conditions	Have the files downloaded on their device.
Post-conditions	User is on the html page of the animation they selected
Basic Flow	1. User opens tool on the homepage 2. User clicks Animation one
Alternative Flow	1. User opens tool on the home page 2. User clicks Animation two/three/four/five/six

UML Diagram of Use Case 1



3.9 Risk Assessment

ID	Risk Type	Risk Description	Likelihood (0-5)	Impact (0-5)	Total (Likelihood*hood)	Mitigation Response
I.	Project	Physical loss of work and therefore progress made.	1	5	5	Regularly take backups of project code and written work. Store the back-ups on a separate device at a different location.
II.	Project	Becoming unwell as a result of Covid-19 and as a result the project becoming behind.	3	4	12	This has been given a higher likelihood rating than normal due to current health situation of Covid-19 in the UK right now. Therefore, as a mitigation I will try to allow time for setbacks due to illnesses and as a last result If I become unwell, I will apply for an extension that is available if a student becomes unwell due to Covid-19.
III.	Project	Change of Project scope	1	2	2	If this occurs, then any reasons for a change will be fully justified within this portfolio. Regular meetings will be held with my supervisor to monitor and discuss any needed changes to the project scope.
IV.	Performance	Implementation stage taking longer due to lack of experience with creating an animation and the chosen languages	3	3	9	If this is the case, then the easter break three-week period can be used to restore the project to its timeline.
V.	Technical	Disruption to the project due to hardware and software issues such as computer breaking or unable to download any necessary software.	1	4	4	All required software and needed programming libraries will be downloaded and tested in the early stages of project, to ensure these issues are discovered in time before the project is implemented. If my computer fails, I will seek to loan one from the university, loss of work due to hardware problems is covered by risk one.

4. Implementation

During the entirety of the implementation, I tried to adhere to best coding practices that I have learnt throughout my degree and placement year as a developer. This entailed using variable names that are descriptive where needed to allow for someone else reading the code to be able to follow and understand what variables are for. Additionally, structuring code neatly and indented in standard practice that helps identify what code lies within loops or within functions. Lastly, providing comments to significant areas where needed to explain what is happening within parts of the code that are not as apparent on reading the code alone.

As discussed in the design section the structure for my code consists of html, css and JavaScript files. In total I have 7 html pages, one for the home page and one for each of the six animations I created. Each of the six html pages had its own JavaScript file with providing the page with its functionality. I made use of anime.js library that provided a wealth of documentation that I found incredibly useful in helping me teach myself from scratch how to code such features. Shortly I will show the features used from the documentation.

The last of the files I created was for the styling. I created a CSS style sheet that was the first core style sheet then from there each html file had its own CSS file that had CSS changes unique to each file. Through utilising the benefits of Cascading Stylesheets (CSS) I minimised redundant code that would have otherwise been repeated in every CSS file.

The following sections break down each animation into how it was implemented.

4.1 Homepage

This is the homepage I implemented figure 25. Using <h1> and <p> tags I have created the title and welcome text styles in the linking stylesheet.

Then for the 6 buttons I created a div container and within that there is with 6 div containers (figure28). I wanted to make this page animated and through research of button animations I took inspiration from (Coulter, n.d.)[xliii] . Where I created two faces of the cube for each button shown in figure 27. These were then appropriately styled to hover rotate to each face shown in figure 28 and 29. They were very difficult to manipulate in order to have both faces attached so that when they rotate on hover the cube seamlessly rotates with no gap between the two faces. This can be seen in figure 26 of the cube rotating. Then with the use of a onclick="button1()" for example a function is ran in the JavaScript that replaces the window.location with the appropriate html page for each animation.

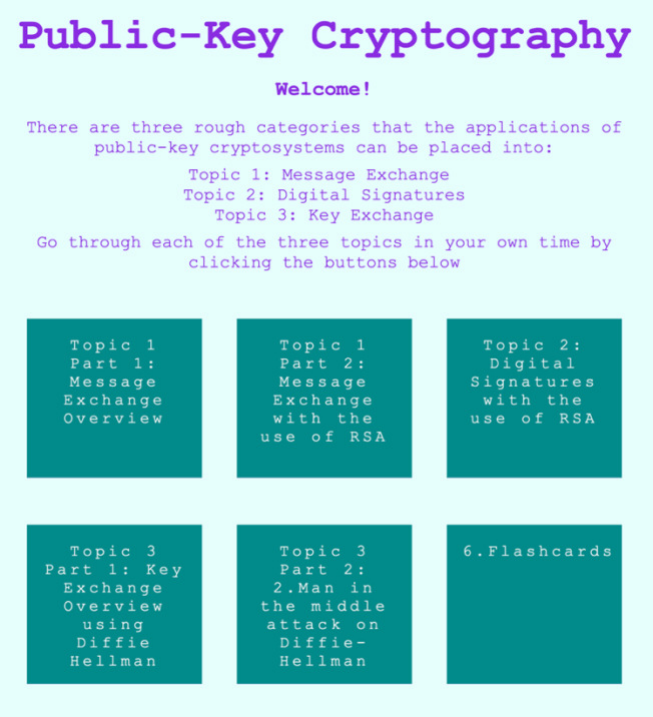


Figure 25 Homepage

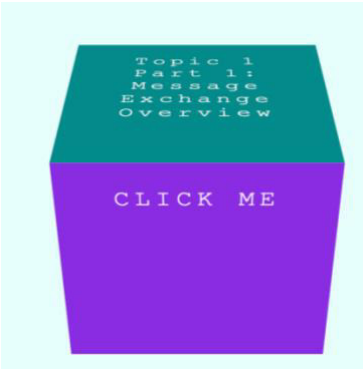


Figure 26 Rotating Button

```
<div id="buttons">
      <div class="spinbutton">

        <div class="cube">
          <div class="face1"> <span class="spany">Topic 1 Part 1: Message Exchange Overview</span></div>
          <div class="face2" id="intro" onclick="button1()"> CLICK ME</div>
        </div>
      </div>

      <div class="spinbutton">
```

Figure 27 Button faces code

```
.spinbutton{
  display: inline-block;
  margin: 20px;
  width: 250px;
  height: 200px;
  perspective: 800px;
  font-family: "Lucida Console", "Courier New", monospace;
  cursor: pointer;
  margin-bottom: 70px;
}

.spinbutton:hover .cube{
  transform: rotateX(90deg);
}
.cube{
  position: relative;
  width: 220px;
  height: 200px;
  margin: auto;
  transform-origin: 50% 50%;
  transform-style: preserve-3d;
  transition: 0.4s all;
}
```

Figure 29 CSS for rotating button

```
.face1{
  position: absolute;
  width: 100%;
  height: 100%;
  background: darkcyan;
  vertical-align: middle;
  text-align: center;
  color: white;
  font-size: 20px;
  padding-top: 22px;
  padding-left: 20px;
  padding-right: 20px;
  letter-spacing: 4px;
  transform: rotateX(0deg) translate3d(0px,0px,100px);
}

.face2{
  position: absolute;
  width: 100%;
  height: 100%;
  background: blueviolet;
  text-align: center;
  color: white;
  font-size: 20px;
  padding-top: 22px;
  letter-spacing: 4px;
  transform: rotateX(-90deg) translate3d(0px,0px,100px);
}
```

Figure 28 CSS for rotating button

4.2 Message Exchange animation

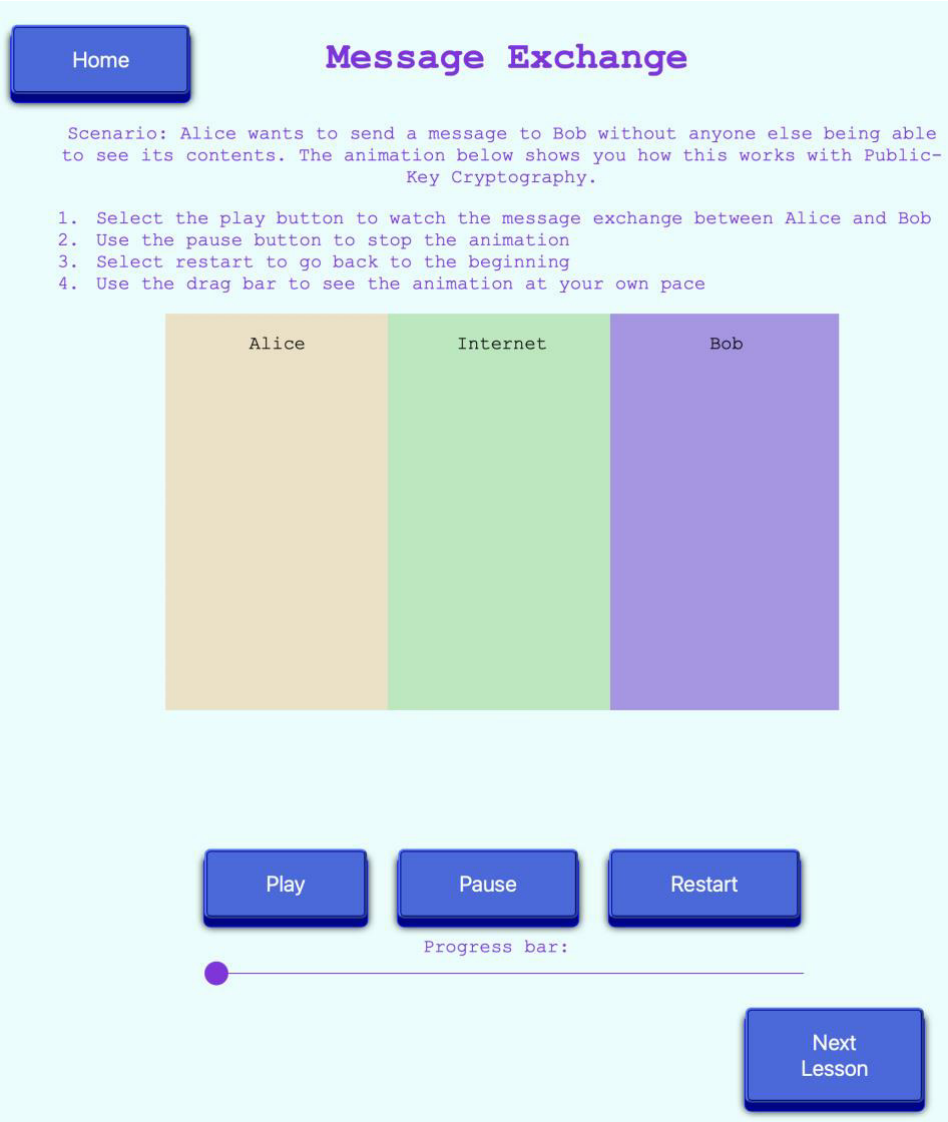


Figure 30 Message Exchange animation

Figure 30 shows the animation for a message exchange, to create this I have a central div container within that I have created four horizontal block divs that through css are styled to dive into 3 colours with a harsh gradient showing clear lines of colour without blending. They are divided into lines so that I could hold different images within each vertical line that move across the screen.

The Controls I have made through creating three <button> 's and a<input> element as a range drag bar, that is linked to JavaScript to match the timeline of the animation, shown in figure 31.

```
<div class="controls">
    <button class="play">Play</button>
    <button class="pause">Pause</button>
    <button class="restart">Restart</button>
    <p id = "seek">Progress bar: <input class="seek" step="1" type="range" min="0" max="100" value="0"> <span class="seek-value"></span></p>
</div>
```

Figure 31 Code of controls on animation

Below the coloured column there is a div container that holds 8 pieces of text all overlapping each other, through the anime.js timeline I created they each fade in and out through using the visibility variable

set to either 0 or 1, as the animation progresses. Similarly, each image of a key or lock for example was placed onto the central div using CSS padding and margins to place it in the correct starting position.

Figure 32 shows how I created a timeline which is triggered when the user clicks play. I then added each movement or transition to this timeline by using the .add() I can add every element to fade in, out, translate on screen and much more. This is done by using the "targets" variable to choose which element from the html page to add the motion too, "opacity" to be visible or invisible, "easing" to have different forms of movement, "duration" dictating how long for and "translate or translate" to cause movements of the object . Each element of movement I created through the use of the timeline and Figure 33 shows the images I placed onto the screen and would be translated, the text below uses inline styling to match the text with the keys, further helping the user to follow what is happening. This animation took approximately 260 lines of code to perform each movement required as part of showing a message exchange between Alice and Bob.

```
const timeline = anime.timeline({
  duration:3000,
  loop:false,
  autoplay:false,
  easing: 'easeInOutSine',
});

timeline.add({
        targets: '.text0',
        opacity: [0,1],
        easing: "easeInOutQuad",
        duration: 1250,
      },'+=300')
```

Figure 33 Creating a timeline code

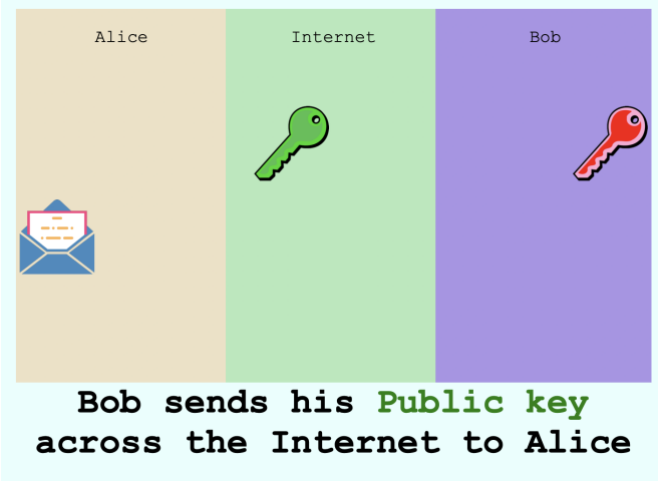


Figure 32 Movement of the animation

The Key Exchange Overview with Diffie-Hellman and Man-in-the-Middle animation were constructed with the same core coding functions and set up, they can be seen in the Appendix (Item 1 and Item 2)

4.3 Message exchange with RSA Mathematics & Digital signatures with RSA Mathematics

Here I will go through the Digital Signatures animation in detail, the Message Exchange mathematics animation can be found in the appendix (Item 3) as the implementation in both is very similar in nature I will only go through one in depth.

For the final implementation of the digital signature's animation, it is difficult to show the main features within image format, as the bulk of the implementation is in the movement and animated effects. From Figure 34, you can see the entirety of the text presented to the user by the end of the animation, these text elements gradually appear as the user progresses through the animation.

Home

Digital Signatures with RSA

Let's now look at how to use Public-Key Cryptography with RSA to create digital signatures for message authentication between Alice and Bob.

Click each step to progress through the process.

Scenario: Bob wants sends a message to Alice, as well as a digital signature so Alice can authenticate that the message was sent by him.

Alice	Internet	Bob
$k_{pub}=(33,3)$ (5, 14) Now to Verify Bob's Signature! Step 1: Alice calculates the digital signature herself x' by $x' = s^e \bmod n$ $x' = 14^3 \bmod 33 = 5$ Step 2: Alice compares her digital signature x' to Bob's digital signature x mod n If x'= x mod n --> Valid Signature If x' != x mod n --> Invalid Signature x' = 5 AND 5 mod 33 = 5 Therefore it is a valid Signature, because x' is equal to the result of x mod n. Conclusion: Alice now knows it is a valid signature therefore, Bob generated the message. This means it has not been altered in transit. Message authentication and message integrity are provided.		Step 1:Choose two prime numbers p and q p = 3 and q = 11 Step 2: Calculate n by p x q n = 3 x 11 = 33 Step 3: Calculate $\Phi(n)$ by (p-1)x(q-1) $\Phi(n) = (3-1)\times(11-1) = 20$ Step 4: Select the public exponent e such that the GCD of and $\Phi(n) = 1$ e = 3 Step 5: Compute the private key d such that $d \equiv e^{-1} \pmod{\Phi(n)}$ $d \equiv 3^{-1} \bmod 20 \equiv 7$ Bobs Public Key is: $k_{pub} = (n, e)$ $k_{pub} = (33,3)$ Send Public Key to Alice Step 6: Choose Bob's message x Message: 5 Enter Your message to compute signature on is: 5 Step 7: Generate Signature s by $x^d \bmod n$ $s = sig_{k_{pr}}(x) \equiv 5^7 \bmod 33 \equiv 14$ Step 8: Send message and signature to Alice (5 ,14)

Previous Lesson

Next Lesson

Figure 34 Digital signatures animation

The processes for creating this animation were to create the template for this page based on the previous animation to ensure familiarity to the user. I then created all of the text elements and placed them onto the appropriate div rectangles. This involved a lot of pain staking manipulation of margins, padding, displaying objects as absolute or relative. Often one changing throwing the whole positioning of neighbouring elements off. Once I placed all textual elements on the animation I began work on the JavaScript file. Where I used the code shown in figure 35 to make each <p> element of text on the html page clickable to cause an animation to trigger. When the user clicked a text step this code would cause the appropriate timeline to play.

```
var first = document.getElementById('first');
first.addEventListener('click', function(){
    timeline.play();
})
```

Figure 35 Code to make text clickable

This is where I then coded each small timeline to take place, I structured this animation like this so a user could go through the mathematics at their own pace and only view the next piece of information when they were ready. It also promotes recall learning as the user can try to remember what the next step will be before the click it, if it's not their first time using this animation.

The process of creating the timeline varied on the stage of the lesson. If we first look at a simple text step as part of the key generation. For Step 2 the Text Reads "Step 2: Calculate n by p x q", when the user clicks this step the text of "n = p x q" fades in within my timeline, next I coded the individual p and q to fade out by placing them within a tag in the <p> element they were in. By giving the a unique id I can remove part of the paragraph sentence. Once I faded these out in the timeline next, I had individual "3" and "11" text in a div element overlaying where they are shown in step 1 so that these can then fade in and be translated to where "p" and "q" were originally. This shows the user where 3 and 11 came from and how they are now placed into the equation of the values for "p" and "q" to then times together to reveal "=33" that fades in. Lastly, as part of this timeline I added the text for Step 3 to fade in which is the next element the user can click.

In order to successfully position these numbers and movements it took a great deal of manipulation and repeated checking of the coordinates I was translating by to ensure it arrived in exactly the correct position. The nature of the code did not result in being lengthy it was however extremely time consuming and labour intensive, as this process was repeated, and a unique timeline created for every step clicked.

Once the user reaches the stage of clicking "Send Public Key to Alice" there is a new nature of animation I created. Through creating a <svg> I created a <path> within a <viewbox> that allowed me to plot a route for the Public key to follow" in the html (figure 36) and then declared a anime.path within the JS. This again was something very difficult to implement. I used (SvgPathEditor, n.d.)[xliv] shown In figure 40 to plot a path which I was unable to see if was suitable until I ran it on my animation, where I would then have to adjust the start and end points and flow of the route to match the other elements on the screen, each time the path was changed I would need to refresh and re-manipulate the route until it worked on the html page. Manipulating the viewbox size also took some time to finalise as changes would cause how much of the path was being chopped off. Once the path was how I wished it to be I made the line not visible and worked on attaching my key text to it. To do this I created the Public key as a <p> element that would first fade in as part of the timeline and I encountered a problem that the text is automatically upside-down on the route, to combat this I rotated it first within the JS code before transforming it along the route (figure 37) , figure 38 and 39 shows it moving in the animation.

```
<div class="pathtoalice">
    <svg  viewBox="-900 -250 418 253" ><path d="M -220 -105 C -793 -35 -426 -370 -584 -473 C -748 -679 -370 -736 -972 -746" stroke=
    <div class="route"><div class="text"><p>k<sub>pub</sub>=(<span class = "nstyle">33</span>,<span class = "estyle">3</span>)</p>
</div>
```

Figure 36 Plotting of path in code

```
timelinePath.add({
        targets: '.text',
        opacity: [0,1],
        rotate:180,
        duration: 1400,
        easing: 'easeInOutSine',
        autoplay: false
      })
      .add({
    targets: '.route',
    translateX: path('x'),
    translateY: path('y'),
    rotate: path('angle'),
    easing: 'linear',
    duration: 5000,
    loop: true
  } '+=400') add({
```

Figure 37 Code showing each movement in the timeline

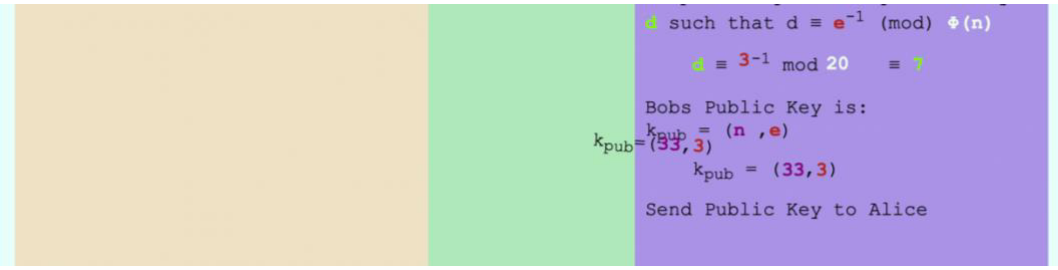


Figure 38 Public Key starting its route

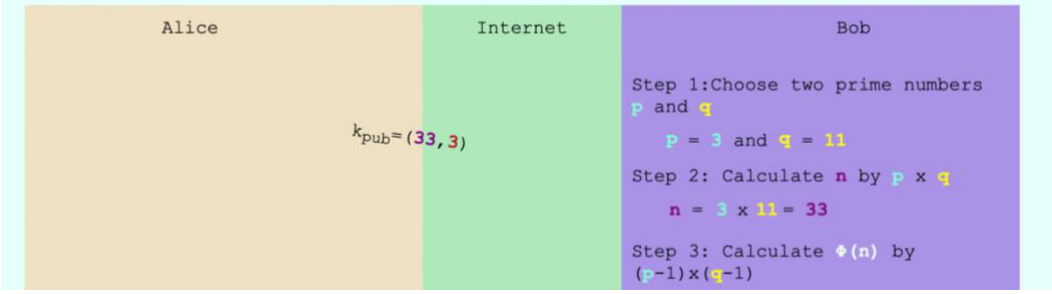


Figure 39 Public Key later on in its route

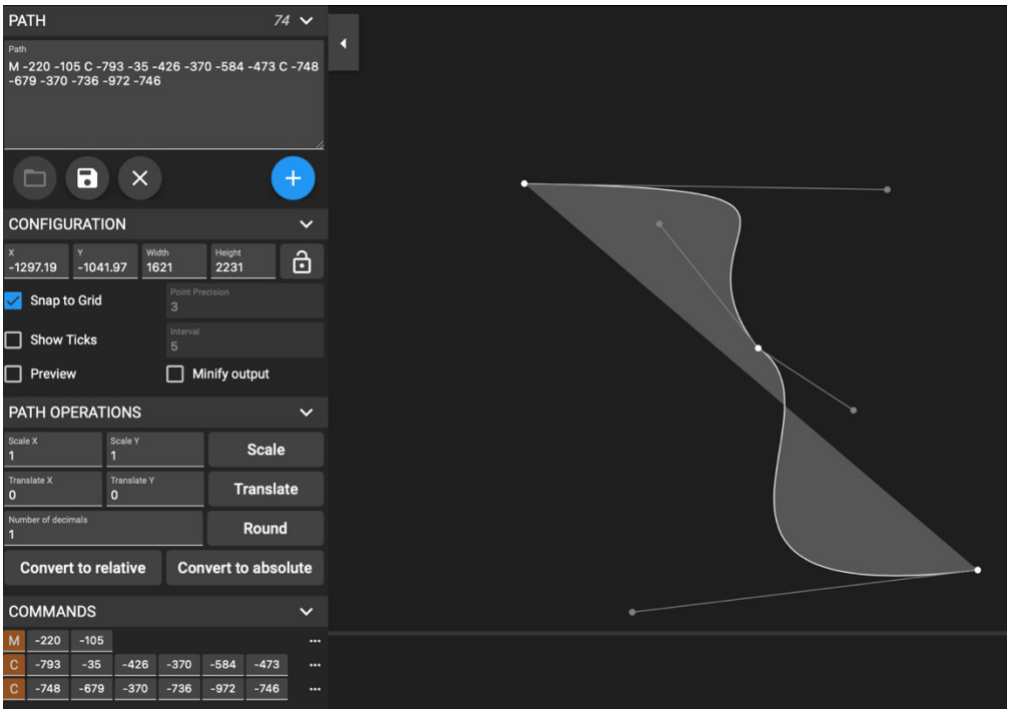


Figure 40 SVG Path Editor

The next step for the user after sending the Public Key to Alice is to enter Bob's message that he wants to send with a digital signature. to implement this I created a input box with a button to allow for the user to enter the button Figure 40. This allowed the user to type in a number or use the arrows on the input box to increment a number figure 42.

```
<p id="entry"> Message: <input type="number" id="myNumber" ></p>
<button id="enterbutton" type="button" onclick="enterX()">Enter</button>
```

Figure 41 Code of button creation

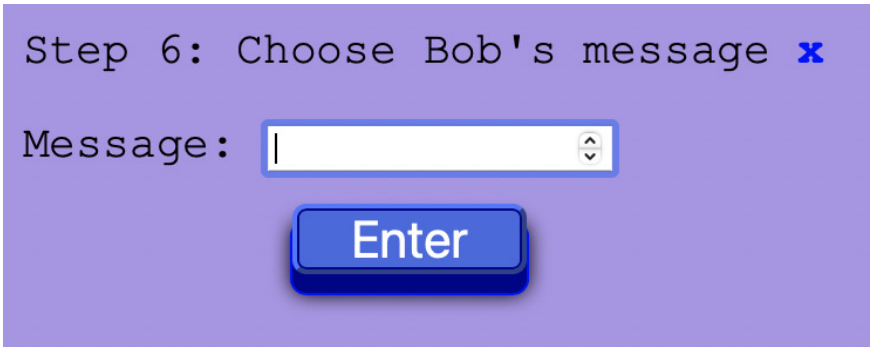


Figure 42 User input box

Figure 43 shows the validation I put on this entry box to ensure as per the rules of RSA in Public-Key Cryptography a message x can must be greater then or equal to zero and less than n-1 (n in my example is 33 so the if statement checks it is less than 33.

```
var x = document.getElementById("myNumber").value;
var validnumbers = /^[0-9]+$/;
if(x.match(validnumbers) && x<33 && x>=0){
```

Figure 43 Validation on User input

Once the user has input their valid input (a message is displayed telling Input not valid, x needs to be a number greater then 0 and less than n if they do not) the next step is displayed. The generation of the signature is animated in the same manner as those discussed earlier and then that too is selected by the user to be sent to Alice. This is where I created a second route path within the html and JavaScript to send that to Alice (figure 44). As these numbers change based on the user input, I used the JavaScript to alter the contents of the created <p> elements. Based on the users input several locations of the mathematics are affected, I used the .getElementById to then reference the appropriate id in the html document and place either the users value x into that or the result of x^emod n dependent on the stage in the mathematics of RSA. This can be seen in figure 45.

```
<div class="pathtoalice2">
    <svg viewBox="-900 -250 418 253" ><path d="M 122 87 C -159 123 -262 -67 -242 -312 C -212 -905 -255 -892 -587 -899" stroke="none" st
    <div class="route2"><div class="text2"><p> (<span class = "xstyle" id="xfill"></span>, <span class = "sstyle" id="sfill"></span>)</

</div>
```

Figure 44 Second route created to send the Digital Signature

```
function enterX() {
  sigtimeline.play();

  var x = document.getElementById("myNumber").value;
  var validnumbers = /^[0-9]+$/;
  if(x.match(validnumbers) && x<33 && x>=0){

    var currentVal = x;
    var xtopower = Math.pow(currentVal,3);
    var mod = xtopower % 33;
    var bobdecrypt = Math.pow(mod,7)%33;
    var result = Math.pow(x,7)%33;

    document.getElementById("demo").innerHTML = x;
    document.getElementById("xnum").innerHTML = x;
    document.getElementById("xnum2").innerHTML = x;
    document.getElementById("equalssig").innerHTML = result;
    document.getElementById("resultsig").innerHTML = result;
    document.getElementById("xfill").innerHTML = x;
    document.getElementById("sfill").innerHTML = result;
    document.getElementById("aliceS").innerHTML = result;
    document.getElementById("aliceX").innerHTML = Math.pow(result,3)%33;
    document.getElementById("aliceX2").innerHTML = Math.pow(result,3)%33;
    document.getElementById("bobX").innerHTML = x;
    document.getElementById("lastsum").innerHTML = x%33; ;

  } else {
    text = "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)";
    document.getElementById("demo").innerHTML = text;

  }
}
```

Figure 45 Validation on user input box and then mathematics replacing the correct numbers in html

After the message and signature is sent to Alice the user can click through the remainder of steps that show the user if the message is indeed a valid signature.

Figure 47 shows the final page of the animation learning tool. It is the flashcards page, as visible from figure 47 there are 16 flashcards that recap and provide some new information to the user. Figure 46 shows the flashcards once some have been rotated. To rotate each flashcard the user can hover over a flashcard where there cursor will change to a clickable pointer to indicate it can be clicked. Then on clicking the flashcard it will rotate round to show the user the answer displayed in a different colour.

Figure 47 Flashcard's page

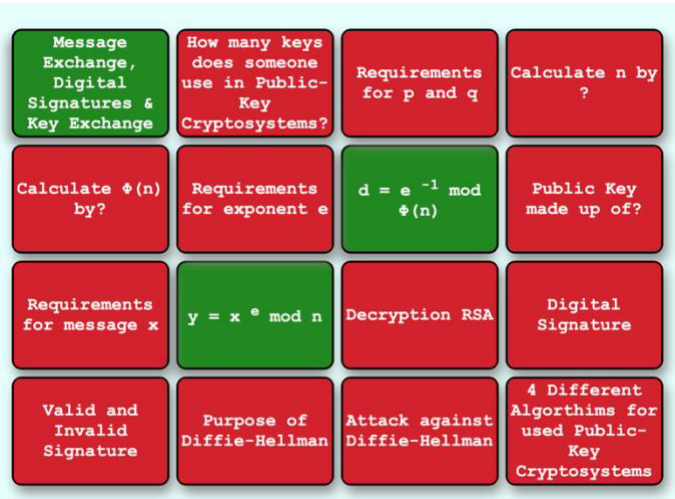


Figure 46 Flashcards once clicked

To create this page, I found inspiration of a card flip which is commented within my code. The code itself did not work and was a demo of one card only. I modified this code to make it work and to create a grid of cards.

Within my html document I created a div container with CSS styling to make it into a grid to display cards evenly in rows. Then within that div container I created a div container for each individual card which had the text given for the front and back of the card as shown in figure 48. CSS styling was used to style the front and back to be different colours and matching sizes.

```
<div class="cardBox">

  <div class="card0">
    <div class="front">
      <p>3 applications of Public-Key Cryptosystems</p>
    </div>
    <div class="back">
      <p>Message Exchange, Digital Signatures & Key Exchange</p>
    </div>
  </div>
```

Figure 48 Html code for each flashcard

Then within the JavaScript for each card I created a variable (figure 49) that could be selected and when it was selected it ran the function shown in figure 50. Figure 50 shows code that runs an anime timeline in which its targets are only the one card, the scale dictates how dramatic and zoomed in and out the card flip looks, rotate rotates the card around the Y-axis, easing is the animation effect, and the duration dictates how long the card takes to rotate.

```
var card0 = document.querySelector(".card0");
```

Figure 49 Declaring a card in JavaScript

```
card0.addEventListener('click',function() {
  anime({
    targets: card0,
    scale: [{value: 1}, {value: 1.5}, {value: 1, delay: 300}],
    rotateY: {value: '+=180', delay: 200},
    easing: 'easeInOutSine',
    duration: 450
    });
});
```

Figure 50 anime timeline function for each card flip

4.5 Challenges faced and techniques used

In the implantation of this project there were a lot of challenges to create movements within the JavaScript and styling in CSS to make all the movements and layout of objects perfect. This caused an enormous amount of continuous small changes needed to be made to perfect the animations. A useful tool I used to combat having to made constant refreshes to code is to use the inspect source code tool available within the browser. Figure 51 shows the features that I most commonly used. It allowed me to view each html element such as divs and see what CSS was being applied and transform movements, both of which I could live edit, remove and add to see what affect this had to the element itself and the whole page. Then once I found what worked I could then make this change permanent within my code.

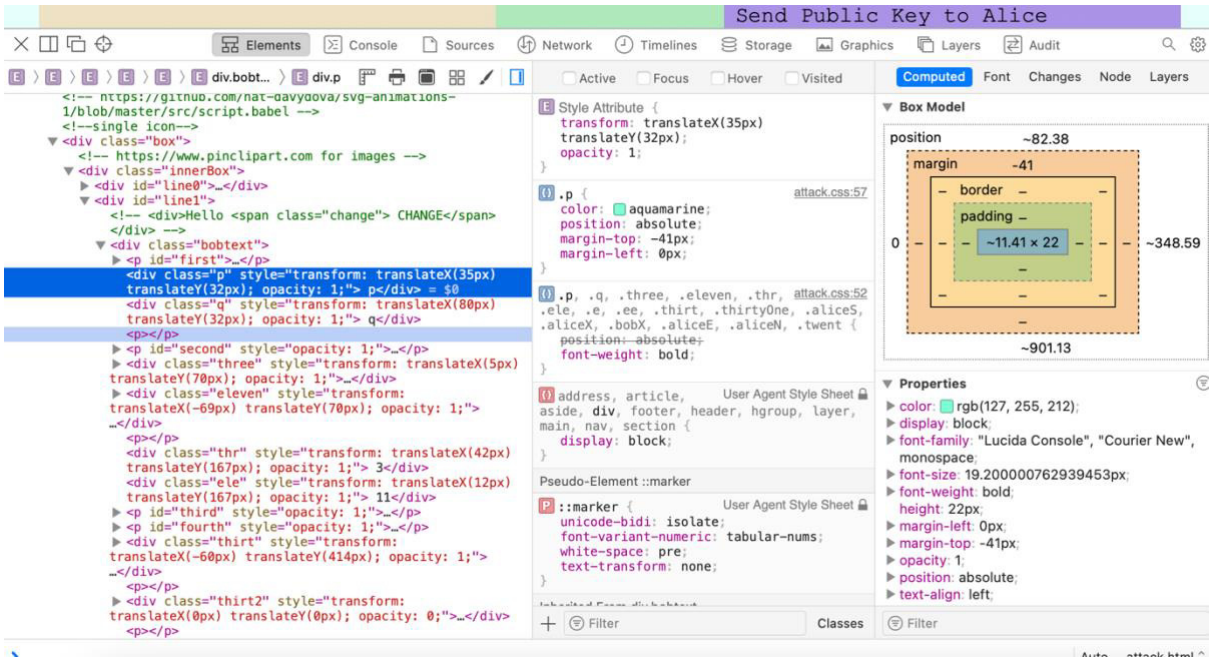


Figure 51 Inspect tool on browser

This was significantly helpful when trying to make my page responsive to window size changes which I did accomplish. As this is something that's very important to have adaptable to different users window sizes and took a great deal of time to adjust and some refactoring of code when realising not everything was working with window resizes.

Other tools I used in the implementation was Preview on Mac to edit images which included annotating such as shown in figure 52 where I wrote "Eve" on the image. Additionally, I used this to label keys in the Diffie-Hellman animation for example.

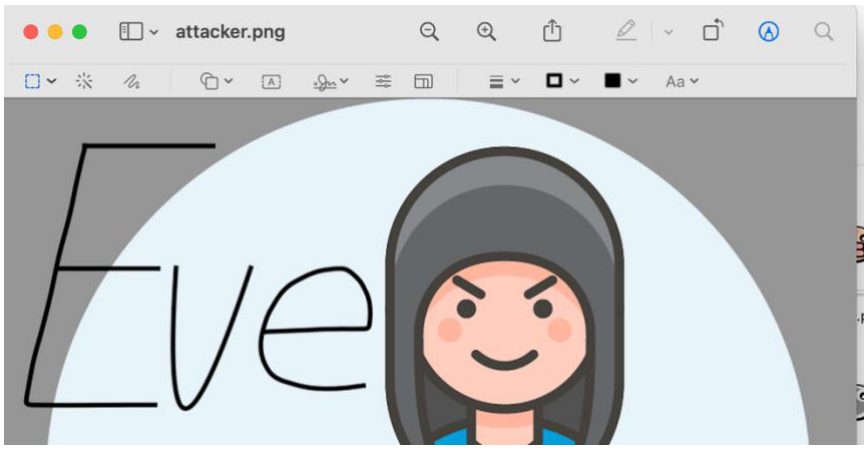


Figure 52 Using Preview to annotate images

As a whole the implementation was very challenging due to the intricate nature of all the small movements and changes in coordinates to styling to make the animations run smoothly. This caused the process to be very labour intensive and time consuming. More time was spent on implantation than initially planned (i.e. the Easter Break period which was scheduled for Holiday). However, as a result of all the time spent each animation is responsive to window changes, has smooth movements and the tool as a whole is fully extensible. A new animation can be added on as its separate html, CSS and JavaScript files with an addition of a new linking button on the homepage. The future of extending this animation tool was kept in mind throughout the implementation of this project.

5. Results & Evaluation

5.1 MOSCOW Requirements Evaluation

Requirement Number	Requirement Description	Requirement Type	Acceptance Criteria	Requirement Met
1.	There must be a working homepage	Must	Yes/No	Yes
2.	There must be at least one animation dedicated to each of the three applications of Public-Key Cryptography (Message Exchange, Digital Signatures and Key Exchange	Must	Yes/No	Yes
3.	The tool must have a consistent colour scheme and layout	Must	Yes/No	Yes
4.	The tool must have interactive elements for the user on every animation	Must	Yes/No	Yes
5.	The tool must run on Windows and Mac operating systems.	Must	Yes/No	Yes
6.	There should be an interactive flash card feature	Should	Yes/No	Yes
7.	There should be an animation showing a man in the middle attack on Diffie-Hellman Key Exchange	Should	Yes/No	Yes
8.	There should be an animation showing the mathematics behind a message exchange with RSA	Should	Yes/No	Yes
9.	There should be an animation showing the mathematics behind Digital Signatures with RSA	Should	Yes/No	Yes
10.	The system should not have any error pages generated	Should	Yes/No	Yes
11.	The system should base timings of reading animated text on average user reading times.	Should	Yes/No	Yes
12.	The system could have colour coding for different variables.	Could	Yes/No	Yes
13.	The system could have an animation showing the mathematics behind a key exchange and man in the middle attack	Could	Yes/No	No

5.2 Test Cases checking functionality

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
1.	User Opens and runs the code on a Windows Computer	The code is downloaded on a Windows machine	Open the homepage html	All Code	Home page loads successfully	Home page loaded successfully	Pass
2.	User Opens and runs the code on a Mac Computer	The code is downloaded on a Mac machine	Open the homepage html	All Code	Home page loads successfully	Home page loaded successfully	Pass
3.	Home Page Buttons Rotate	Be on the home page	Hover mouse over each of the six buttons	Home page	Each of the seven buttons rotates round to the second face when hovered over	Each of the seven buttons rotated round to the second face when hovered over	Pass
4.	Home Buttons	Be on the Homepage	1. Click Animation 1 2. Click the Home button 3. Click Animation 2 4. Click the Home Button 5. Click Animation 3 6. Click the Home button 7. Click Animation 4 8. Click the Home Button 9. Click Animation 5 10. Click the Home button	Every html page	Each of the 6 times the home button is clicked the html of the homepage is loaded	All 6 times the home button was selected the home page was loaded	Pass

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
			11. Click Animation 6 12. Click the Home Button				
13.	Next Button	Be on the first animation page	Click the Next Button 5 times	Every animation page	Each time the next button is clicked the next animation page is loaded with no repeating pages, should finish on flashcard page where there is no next button.	Every time the next button was clicked the next animation page was loaded and there were not any repeating pages. The next button was not visible on the final page.	Pass
14.	Previous Button	Be on the last animation page (flashcards)	Click the Previous button 5 times	Every animation page	Each time the previous button is clicked the previous animation page is loaded with no repeating pages, should finish on first animation page where there is no previous button.	Every time the previous button was clicked the previous animation page was loaded and there were not any repeating pages. The previous button was not visible on the first page.	Pass
15.	Play, Pause, Restart Button on Message Exchange animation	Be on the message exchange animation page	Click Play, wait 30 seconds, click pause, click restart	Message exchange animation	When play is selected and waiting for 30 seconds the animation plays with moving elements happening, when pause is selected everything freezes, when restart is selected the animation goes back to the beginning.	When play was selected the animation played with moving elements happening, when pause was selected everything freezes, when restart was selected the animation went back to the beginning.	Pass

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
16.	Play, Pause, Restart Button on Key Exchange animation	Be on the Key Exchange page	Click Play, wait 30 seconds, click pause, click restart	Key exchange animation	When play is selected and waiting for 30 seconds the animation plays with moving elements happening, when pause is selected everything freezes, when restart is selected the animation goes back to the beginning.	When play was selected the animation played with moving elements happening, when pause was selected everything freezes, when restart was selected the animation went back to the beginning.	Pass
17.	Play, Pause, Restart Button on Man-in-the-middle attack animation	Be on the Man-in-the-middle attack animation	Click Play, wait 30 seconds, click pause, click restart	Man-in-the-middle attack animation	When play is selected and waiting for 30 seconds the animation plays with moving elements happening, when pause is selected everything freezes, when restart is selected the animation goes back to the beginning.	When play was selected the animation played with moving elements happening, when pause was selected everything freezes, when restart was selected the animation went back to the beginning.	Pass
18.	Progress Bar on Message Exchange animation	Be on the message exchange animation page	Drag the circle on the progress bar forwards to the end and then back to beginning.	Message exchange animation	When the drag bar is moved the animation movement occurs at the speed the bar is dragged to full completion when the bar is at the end and then live goes backwards to the start when the bar is moved back to the beginning.	The animation did progress live with the movement of the bar to full completion and then back to the beginning in reverse when dragged back to the start of the drag bar.	Pass

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
19.	Progress Bar on Key Exchange animation	Be on the Key Exchange page	Drag the circle on the progress bar forwards to the end and then back to beginning.	Key exchange animation	When the drag bar is moved the animation movement occurs at the speed the bar is dragged to full completion when the bar is at the end and then live goes backwards to the start when the bar is moved back to the beginning.	The animation did progress live with the movement of the bar to full completion and then back to the beginning in reverse when dragged back to the start of the drag bar.	Pass
20.	Progress Bar on Man-in-the-middle attack animation	Be on the Man-in-the-middle attack animation	Drag the circle on the progress bar forwards to the end and then back to beginning.	Man-in-the-middle attack animation	When the drag bar is moved the animation movement occurs at the speed the bar is dragged to full completion when the bar is at the end and then live goes backwards to the start when the bar is moved back to the beginning.	The animation did progress live with the movement of the bar to full completion and then back to the beginning in reverse when dragged back to the start of the drag bar.	Pass
21.	Checking the clickable steps on Message Exchange Mathematics animation	Be on the Message Exchange Mathematics animation	Click through the entirety of the animation, when reaching the input box enter a valid input of "5"	Message Exchange Mathematics animation and "5"	Each time a step is clicked an animation is shown of the maths in each step happening and then the next step fading in to be clicked until full completion.	Each time a step was clicked in the animation the moving maths elements were shown then the next step did fade in until full completion.	Pass
22.	Checking the clickable steps on Digital Signatures	Be on the Digital Signatures Mathematics animation	Click through the entirety of the animation	Digital Signatures Mathematics animation and "5"	Each time a step is clicked an animation is shown of the maths in each step happening and then the next step fading in to be	Each time a step was clicked in the animation the moving maths elements were shown then the next step did	Pass

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
	Mathematics animation				clicked until full completion.	fade in until full completion.	
23.	Check User input box on Message Exchange Mathematics animation – valid input	Be on the Message Exchange Mathematics animation and click through the steps to reach the point of the input box showing	Enter 5 into the input box and click enter	“5”	The input is accepted and the number “5” is shown after the text “Your message is:”	The input was accepted and the number “5” was shown after the text “Your message is:”	Pass
24.	Check User input box on Message Exchange Mathematics animation – invalid input	Be on the Message Exchange Mathematics animation and click through the steps to reach the point of the input box showing	Enter 500 into the input box and click enter	“500”	The input is not accepted, and an error message appears telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	The input was not accepted, and an error message appeared telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	Pass
25.	Check User input box on Message Exchange Mathematics animation – invalid input	Be on the Message Exchange Mathematics animation and click through the steps to reach the point of the input box showing	Enter ff into the input box and click enter	“ff”	The input is not accepted, and an error message appears telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	The input was not accepted, and an error message appeared telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	Pass

Test Case ID	Test Scenario	Pre-Conditions	Test Steps	Test Data	Expected Result	Actual Result	Pass/ Fail
26.	Check User input box on Digital Signatures Mathematics animation – valid input	Be on the Digital Signatures Mathematics animation and click through the steps to reach the point of the input box showing	Enter 5 into the input box and click enter	“5”	The input is accepted and the number “5” is shown after the text “Your message is:”	The input was accepted and the number “5” was shown after the text “Your message is:”	Pass
27.	Check User input box on Digital Signatures Mathematics animation – invalid input	Be on the Digital Signatures Mathematics animation and click through the steps to reach the point of the input box showing	Enter 500 into the input box and click enter	“500”	The input is not accepted, and an error message appears telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	The input was not accepted, and an error message appeared telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	Pass
28.	Check User input box on Digital Signatures Mathematics animation – invalid input	Be on the Digital Signatures Mathematics animation and click through the steps to reach the point of the input box showing	Enter ff into the input box and click enter	“ff”	The input is not accepted, and an error message appears telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	The input was not accepted, and an error message appeared telling the user "Input not valid, x needs to be a number greater then 0 and less than n (n = 33)"	Pass
29.	Check Flashcards rotate	Be on the flashcards page	Click Every single flash card to turn it to the other side. Once all flashcards are turned over select them all again to return them back to their original side.	Flashcard’s page	Every flash card should rotate round to the other side and display different text. Then when selected the second time they all rotate back to their original side.	Every flash card did rotate round to the other side and displayed different text. Then when selected the second time they did all rotate back to their original side.	Pass

5.3 User Testing

As part of results, I was due to test the made animations with user testing. This was to cover the objectives of "to determine ease of use of the animation, navigation flow and other functionality conditions." and "to establish whether the tool enhanced users understanding of the subject area."

In order to facilitate this testing, I needed to have finished the development of the entire system before being able to create the user questionnaire as the questionnaire would be specific to which animations were made and the interactive elements placed on each animation. Upon completion of my animation, I submitted a request for ethical approval for my user questionnaire, unfortunately due to the nature of the meetings only being convened fortnightly and being unaware when those meetings were scheduled I discovered I had narrowly missed a fortnightly meeting. I then received feedback days before my deadline of needing to alter application forms which was then impossible to be reapproved in time to conduct testing before the deadline. As a result, it was therefore necessary continue with my evaluation and write up without user testing. User testing will be discussed in future work and reflection of learning in regards of not meeting this objective.

5.4 Evaluation

As a whole I am very satisfied with the outcome of the implementation within this project. First looking at the requirements set out all "Must" requirements have been met, all of the "Should" and all but one of the "Could" requirements have been met. This fulfils the need to complete all must and should then if there was time fulfilling as many as the "Could" as possible.

Moving on to the Test Cases conducted, these were carried out to ensure all functionality within the system works and passed as expected. This included testing user inputs, interactive elements and navigation within the learning tool. All test cases passed showing all the functionality within the system works and 6 successful animations have been made that are combined to give the user a great covered experience on Public-Key Cryptography.

High levels of research went into determining what aids learning and these were considered in the design stage and later implemented. This included the key feature of having play, pause and live rewind to combat the issue of animations on a fixed timer not being able to adapt to each user's needs.

Furthermore, usability was kept in mind throughout the entire creation of this project, this included timings of the animation text being based on average users reading pace, consistent layout and colour scheme and placement of buttons and controls, as discussed in the design section.

The core objective to create an interactive animation has been achieved and, in my opinion, has gone above and beyond to aid in creating an online learning tool that both goes a way towards filling the cyber security knowledge gap identified in my introduction. Furthermore, as I myself have experienced studying my entire final year of my degree having more online learning tools would be great to pass down for university students to use next year in their studies.

Despite not testing on users themselves I am still confident in my animations ability to improve students understanding on the material matter due to including many of the attributes I identified in my research that are known to help in learning and memory retention.

6. Future Work

The first piece of future work that I would conduct would be thorough user testing, since completion of my implementation and submitting for an ethical approval for my original questionnaire I have had time to reflect and think of an improved version that I would use in future work. This questionnaire would have two main sections. Firstly, Section A to ascertain if the users understanding of the subject matter has improved. This would be done by asking users 10 questions on Public-Key Cryptography to gage the users understanding level by scoring their answers. Next show the users the animation and allow them to progress through the entirety in their own pace. Then upon completion of the animations, ask the users the same questions and see if their scores have improved. They key here is to not tell the users how they scored on the first questionnaire to avoid any users recalling previous correct answers. This would allow for quantitative analysis to be done on the results and determine if there was a significant difference of user's knowledge before and after using the animation. Section B of the questionnaire would be based on evaluating the usability of the system which contains 10 questions where answers are predominantly scaled 1 to 10 allowing for quantitative results to be generated and plotted in relation to matters such as usability and ease of use. Once collected these results can be used to evaluate the animation further and make improvements where needed based on user feedback.

When looking at the tool itself there is much more that could be added as the amount of content that could be covered is significant in regards to security education. The way my animations were built was intentionally in a manner that allowed for it to be extendable. If lecturers for example want to show their students the animations I have made but wishes to add how hash functions work they could add another animation by creating a html, CSS and JavaScript file then adding another button on the home page that links to this new animation. All of this would be very achievable without having to manipulate all the other code to allow for a new animation, except adding a home button link. Additionally, if a student next year wishes to extend this for their dissertation they could easily add on the the existing framework to make a more in-depth coverage of security concepts. The nature of the structure has the potential to be a very organised topic by topic sections of animation.

Other future work possibilities would be those I discussed in the "Won't have time" requirements. Which encompassed more complex interactive elements that would have taken significantly more time, as the code examples I researched were very complex and as a complete beginner I did not feel I would have time to implement. This included features such as the user being able to drag and drop items and the system in response telling them if that is correct.

Lastly future work could include having a expert assess the webpage and animations against the heuristics evaluation that I am aware from my studies in the Human Computer Interaction module. An expert would be required to assess against the heuristics, rather than assess against them myself due to my not having had the appropriate training. Upon completion of this evaluation and produced report of faults, improvements could be made to rectify any usability issues raised.

7. Conclusions

In Conclusion this project was targeted at animating security concepts for the purposes of being an educational tool to aid in students learning of security concepts and I believe this has been met. In total 6 animations were made 5 of which are explaining content material and the sixth a teaching and revision tool. From this I have learnt the amount of subject matter on security concepts is very complex and detailed. Therefore, the animations made are not showing the concepts as in depth as the information available through textbooks for example. However, this is something that could be improved on to cover a more in-depth coverage of the subject matter. Although it does give users a very good introduction and enough detail to be able to replicate encryption and decryption of Public-Key Cryptography with RSA as well as an overview of Diffie-Hellman Key Exchange and the Man-in-the-Middle attack.

The main aim of this project as discussed was to create a learning tool to contribute towards filling the gap of knowledge in the UK in the security sector and also to generate further interest in the area through making learning more enjoyable. Additionally, to contribute towards making more online learning resources since students throughout England have been plummeted into learning online from home, where traditional learning sources are not as accessible. Therefore, with respect to these aims I can confidently conclude these aims were met and I believe will be a great example of the possible use of animations to aid in education especially if students learning continues or ever returns to online learning in the future. The aim that was not met was ascertaining whether this animation promoted more enjoyment and interest in the area and to promote people opting to move into the industry, however that has been discussed as not being met due to ethical approval not being achieved in time. Therefore, this will be a part of future work for the project.

8. Reflection of Learning

Looking back over the length of this project I am very pleased with what I have created but additionally with the skills I have learnt throughout the process. At the beginning of this project I had no experience with creating an animation and more specifically with using JavaScript especially, since JavaScript was the key element that created my animation it allowed me to grow my skillset. I am now very confident with the use of JavaScript from its syntax to the functionality it provides when using alongside html and CSS files. I believe this new skillset will help me in my secured Graduate job as it is an additional programming language and genre of work I can apply in future tasks and can add it to my portfolio of expertise I gained from working as a developer in my placement year and from my time at university.

Furthermore, from my research I have enhanced my knowledge of security concepts from my final year module I undertook through reading more in-depth into textbooks on the area. Another key element of my research was about how people learn and what assists with learning and memory retention. This is not something I was previously aware of and will be useful in my future as often in a technology career you have to continuously learn new things and having invaluable insight in how best to improve learning and memory retention could be extremely useful in my future career and studies if choose to undertake further education.

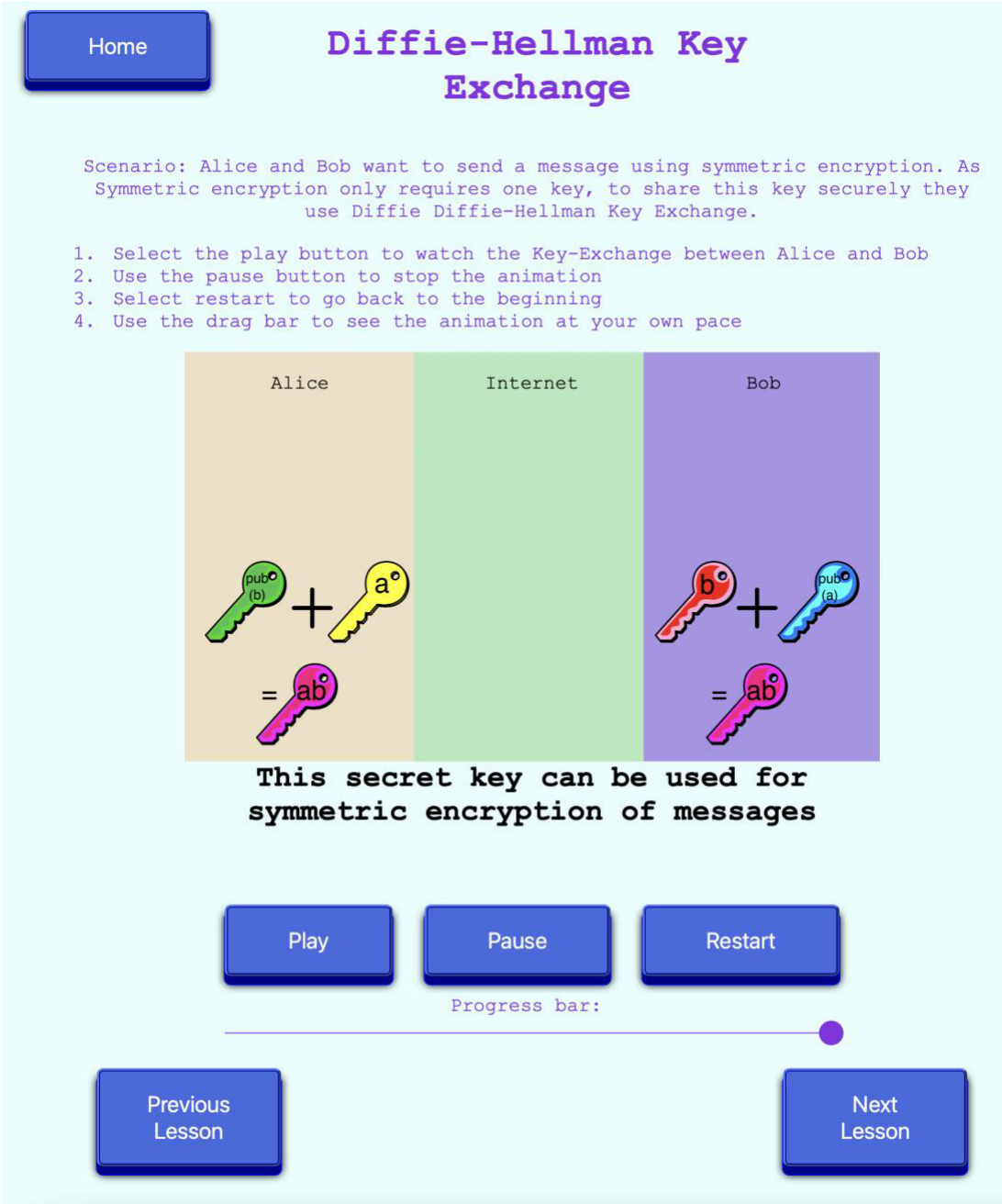
This project has also enabled me to improve my softer skills such as Project Management, Time Skills and awareness of deadlines. As discussed earlier in the report due to ethical approval not being received back in time I have learnt to be more proactive in liaising with other areas/departments that will influence the project. Therefore, in the future if I know my project can be held up by something I will enquire to when I need to submit that information by. This project was a steep learning curve and has made me very aware of being aware of all elements that may affect my project and interfere with the progress, which will be a key learning point going forward into my own career. Therefore, despite it causing a small gap in testing I'm grateful for the teaching points it generated.

I have also gained an appreciation for how a piece of work like this should be organised, developed and written as this is my first large research and development project I have conducted. Throughout the process I needed to make key decisions and learnt when to stop perfecting an animation and move onto the next one.

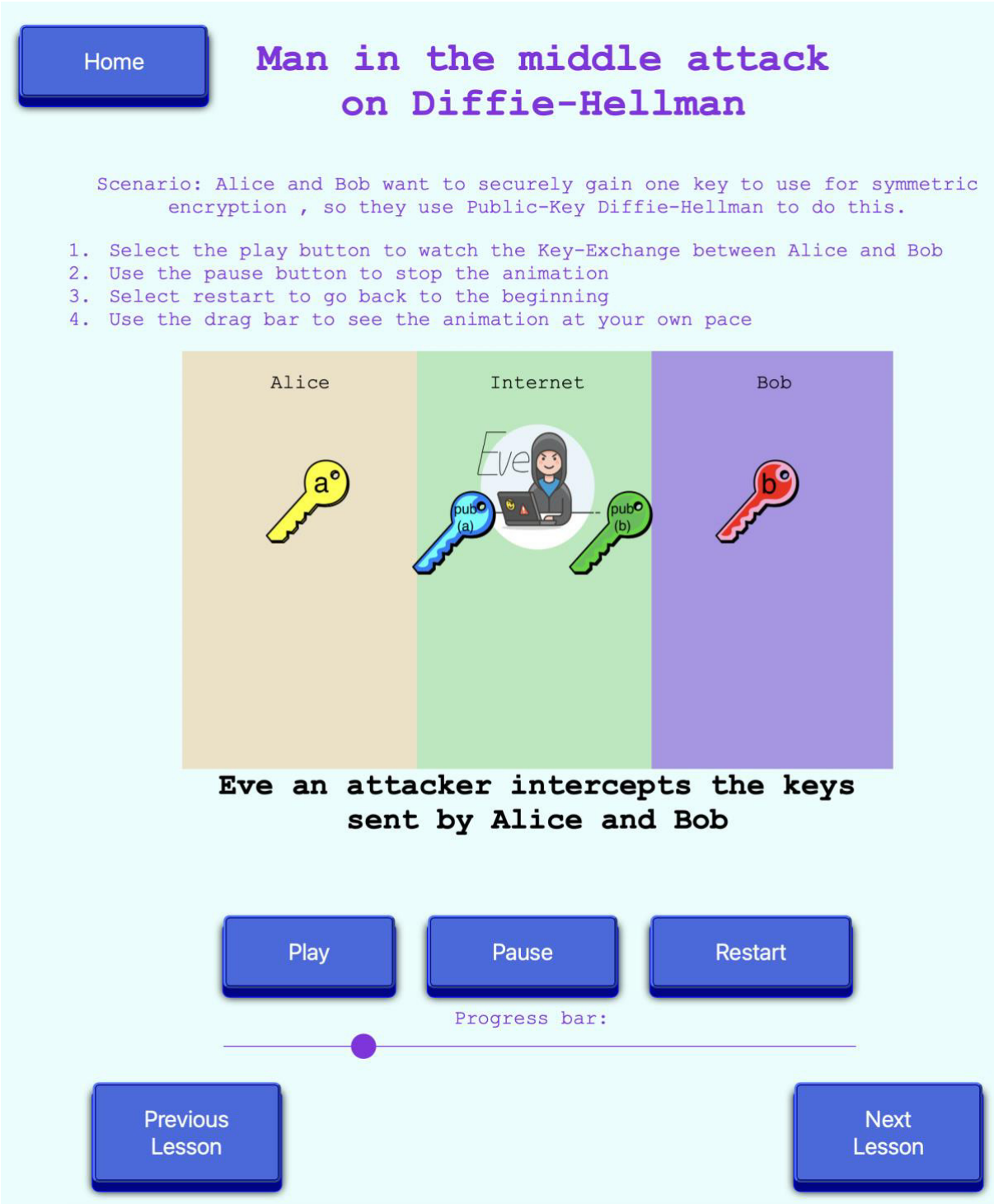
When looking at the project as a whole the frequent supervisor meetings were very useful in keeping me on track with my work and also improving my enjoyment of the project. Due to university being online for my final year it was great to have some interaction in the last few months even if that was just one meeting a week. When going forward after completion of my degree I will take the skills I have learnt from this project and use it as a point of reference to draw on to help me in future projects I undertake.

Finally, I am very happy with the quality of work I have produced in this report and the animation tool that I have made. Each animation was very intricate in the code to make as each small letter or number placement and movement took lots of CSS styling to place and then JS to move. Often one change in the styling would throw everything else off and need redoing. Through perseverance and hard work, I finished 6 animations/learning aids and am very proud of the result.

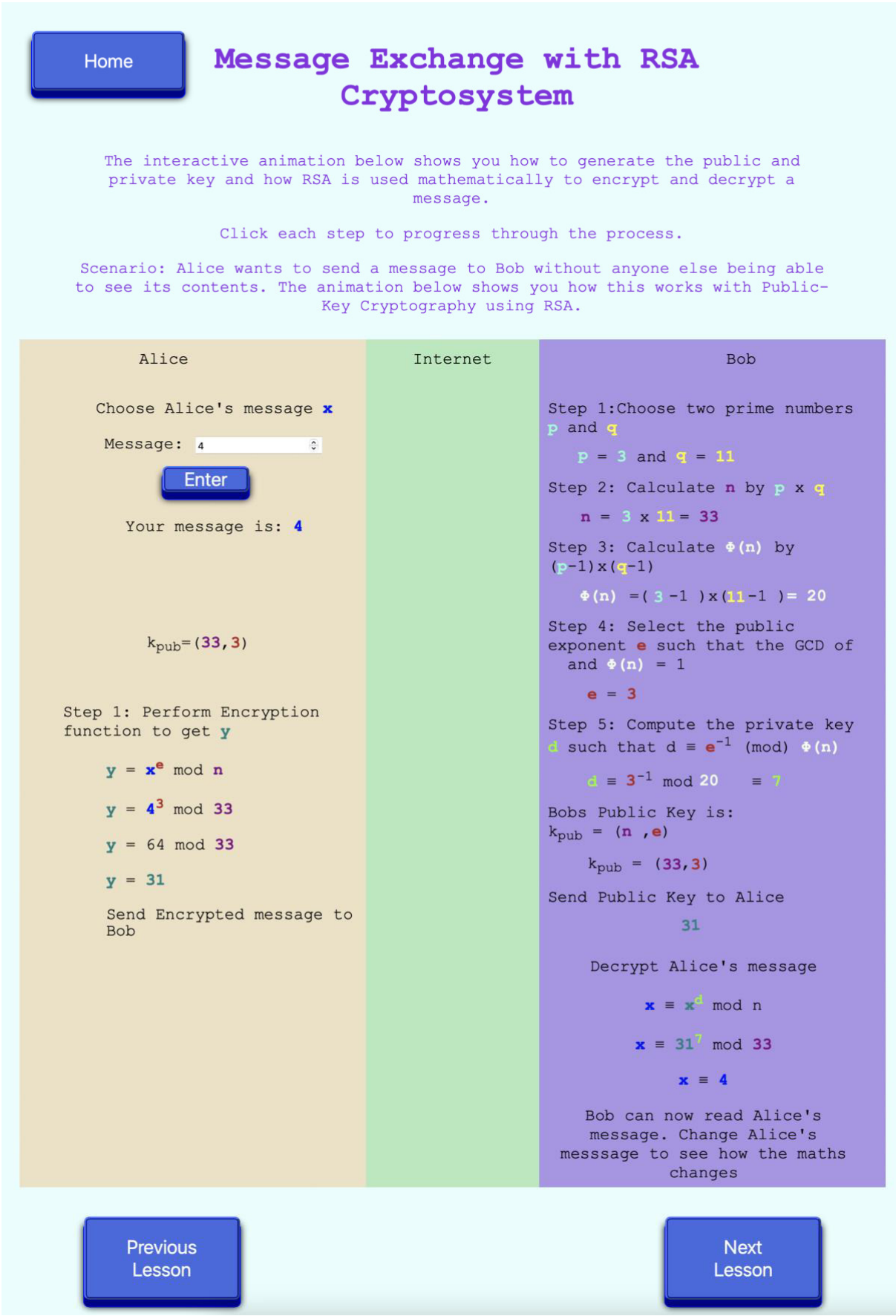
1. Appendices



Item 1 – Diffie-Hellman Key Exchange animation



Item 2 Man in the middle attack animation



Item 3 Message Exchange Mathematics animation

12. References

[i] GOV.UK. Cyber security skills in the UK labour market 2020. [online] Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020?fbclid=IwAR0mAdta1NZtAfjFaGUCWcQQsqjNY58ZTfATOSAXC65aG5Y6d2FTVOpPbSQ

[ii] GOV.UK. Cyber security skills in the UK labour market 2020. [online] Available at: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020?fbclid=IwAR0mAdta1NZtAfjFaGUCWcQQsqjNY58ZTfATOSAXC65aG5Y6d2FTVOpPbSQ

[iii] Oxford Languages (2021). Oxford Languages and Google - English -. [online] languages.oup.com. Available at: https://languages.oup.com/google-dictionary-en/.

[iv] Oxford Languages (2021). Oxford Languages and Google - English -. [online] languages.oup.com. Available at: https://languages.oup.com/google-dictionary-en/.

[v] New York Film Academy. (2017). 5 Types Of Animation: Finding Inspiration In All Styles. [online] Available at: https://www.nyfa.edu/student-resources/5-types-of-animation-finding-inspiration-in-all-styles/

[vi] Alex Safavinia (2020). What is Cel Animation? [online] Marionette Studio. Available at: https://marionettestudio.com/what-is-cel-animation/.

[vii] www.dictionary.com. (n.d.). Definition of 2D animation | Dictionary.com. [online] Available at: https://www.dictionary.com/browse/2d-animation [Accessed 20 Mar. 2021].

[viii] iNurture. (2016). What is 3D Animation? How is it Different from 2D Animation? - iNurture. [online] Available at: https://inurture.co.in/blogs/what-is-3d-animation-how-is-it-different-from-2d-animation/.

[ix] New York Film Academy. (2017). 5 Types Of Animation: Finding Inspiration In All Styles. [online] Available at: https://www.nyfa.edu/student-resources/5-types-of-animation-finding-inspiration-in-all-styles/

[x] New York Film Academy. (2017). 5 Types Of Animation: Finding Inspiration In All Styles. [online] Available at: https://www.nyfa.edu/student-resources/5-types-of-animation-finding-inspiration-in-all-styles/

[xi] Lowe, R. (2004). Animation and learning: Value for money? [online] . Available at: https://www.ascilite.org/conferences/perth04/procs/pdf/lowe-r.pdf [Accessed 21 Mar. 2021].

[xii] Tversky, Barbara, et al. “Animation: Can It Facilitate?” Int. J. Human-Computer Studies, vol. 57, 2002, pp. 247–262, hci.stanford.edu/courses/cs448b/papers/Tversky_AnimationFacilitate_IJHCS02.pdf, 10.1006/ijhc.1017.

[xiii] Tversky, Barbara, et al. “Animation: Can It Facilitate?” Int. J. Human-Computer Studies, vol. 57, 2002, pp. 247–262, hci.stanford.edu/courses/cs448b/papers/Tversky_AnimationFacilitate_IJHCS02.pdf, 10.1006/ijhc.1017.

[xiv] Tversky, Barbara, et al. “Animation: Can It Facilitate?” Int. J. Human-Computer Studies, vol. 57, 2002, pp. 247–262, hci.stanford.edu/courses/cs448b/papers/Tversky_AnimationFacilitate_IJHCS02.pdf, 10.1006/ijhc.1017.

[xv] Malamed, C. (2016). How to Use Animations for Learning. [online] www.td.org. Available at: https://www.td.org/insights/how-to-use-animations-for-learning [Accessed 21 Mar. 2021].

[xvi] Tversky, Barbara, et al. “Animation: Can It Facilitate?” Int. J. Human-Computer Studies, vol. 57, 2002, pp. 247–262, hci.stanford.edu/courses/cs448b/papers/Tversky_AnimationFacilitate_IJHCS02.pdf, 10.1006/ijhc.1017.

[xvii] Oxford Languages (2021). Oxford Languages and Google - English -. [online] languages.oup.com. Available at: https://languages.oup.com/google-dictionary-en/.

[xviii] Ibrahim, M. and Al-Shara, O. (2007). Impact of Interactive Learning on Knowledge Retention. LNCS, [online] II, pp.347–355. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-540-73354-6_38.pdf.
[xix] Ibrahim, M. and Al-Shara, O. (2007). Impact of Interactive Learning on Knowledge Retention. LNCS, [online] II, pp.347–355. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-540-73354-6_38.pdf.
[xx] shiftelearning. (2021). 6 Ways Color Psychology Can Be Used to Design Effective eLearning. [online] Available at: https://www.shiftelearning.com/blog/bid/348188/6-Ways-Color-Psychology-Can-Be-Used-to-Design-Effective-eLearning.
[xxi] shiftelearning. (2021). 6 Ways Color Psychology Can Be Used to Design Effective eLearning. [online] Available at: https://www.shiftelearning.com/blog/bid/348188/6-Ways-Color-Psychology-Can-Be-Used-to-Design-Effective-eLearning.
[xxii] Karpicke, J.D. and Bauernschmidt, A. (2011). Spaced retrieval: Absolute spacing enhances learning regardless of relative spacing. Journal of Experimental Psychology: Learning, Memory, and Cognition
[xxiii] What is retrieval practice (2019). A Powerful Strategy to Improve Learning. [online] A Powerful Strategy to Improve Learning. Available at: https://www.retrievalpractice.org/why-it-works.
[xxiv] Simply Explained (2017). Asymmetric encryption - Simply explained. Simply Explained. Available at: https://www.youtube.com/watch?v=AQDCe585Lnc.
[xxv] Art of the Problem (2012). Public Key Cryptography: RSA Encryption Algorithm. Art of the Problem. Available at: https://www.youtube.com/watch?v=wXB-V_Keiu8.
[xxvi] F. Learning Studio. (2020). 5 EDUCATIONAL ANIMATION EXAMPLES FOR ONLINE COURSES. [online] Available at: https://www.flearningstudio.com/educational-animation-examples-online-courses/
[xxvii] F. Learning Studio. (2020). 5 EDUCATIONAL ANIMATION EXAMPLES FOR ONLINE COURSES. [online] Available at: https://www.flearningstudio.com/educational-animation-examples-online-courses/
[xxviii] R2d3.us. (2019). A visual introduction to machine learning. [online] Available at: http://www.r2d3.us/visual-intro-to-machine-learning-part-1/
[xxix] Guttman, B. and Roback, E. (1995). An Introduction to Computer Security: The NIST Handbook. [online] NIST Publications. Available at: https://csrc.nist.rip/publications/nistpubs/800-12/handbook.pdf
[xxx] Stallings, W. (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE. [online] Pearson. Available at: https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf.
[xxxi] Stallings, W. (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION Hiva-Network.com. [online] . Available at: https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf.
[xxxii] Stallings, W. (2017). CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE SEVENTH EDITION GLOBAL EDITION Hiva-Network.com. [online] . Available at: https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf.
[xxxiii] Interaction Design Foundation (2014). What is Human-Computer Interaction (HCI)? [online] The Interaction Design Foundation. Available at: https://www.interaction-design.org/literature/topics/human-computer-interaction.
[xxxiv] Tutorialspoint. (2019). Guidelines in HCI - Tutorialspoint. [online] Available at: https://www.tutorialspoint.com/human_computer_interface/guidelines_in_hci.htm.
[xxxv] Nielsen, J. (n.d.). Heuristic Evaluation Ten Usability Heuristics. [online] . Available at: https://pdfs.semanticscholar.org/5f03/b251093aee730ab9772db2e1a8a7eb8522cb.pdf.
[xxxvi] Mayer, R.E. (2020). Multimedia learning. 3rd ed. Cambridge: Cambridge University Press.
[xxxvii] Agile Business Consortium (2019). Chapter 10: MoSCoW Prioritisation. [online] Agilebusiness.org. Available at: https://www.agilebusiness.org/page/ProjectFramework_10_MoSCoWPrioritisation.

[xxxviii] Priya (2020). 10+ Best JavaScript Animation Libraries to Use in 2021. [online] CodeinWP. Available at: https://www.codeinwp.com/blog/best-javascript-animation-libraries/.
[xxxix] Priya (2020). 10+ Best JavaScript Animation Libraries to Use in 2021. [online] CodeinWP. Available at: https://www.codeinwp.com/blog/best-javascript-animation-libraries/.
[xl] animejs.com. (n.d.). anime.js. [online] Available at: https://animejs.com/documentation/.
[xli] CodePen (n.d.). CodePen. [online] . Available at: https://codepen.io/trending.
[xlii] Execuread.com. (2012). Speed Reading Facts. [online] Available at: https://secure.execuread.com/facts/.
[xliii] Coulter, D. (n.d.). A Pen by Dean Coulter. [online] Available at: https://codepen.io/jukeboxhero/pen/ggwQzy.
[xliv] SvgPathEditor. (n.d.). SvgPathEditor. [online] Available at: https://yqnn.github.io/svg-path-editor/