Creating a cryptography animation for visual learners
CM3203 - Final Report

Author: Georgina Harvey (1705987)
Supervisor: Dr. George Theodorakopoulos
Moderator: Víctor Gutiérrez Basulto
Module Number: CM3203
Module Title: Individual Project [40 credits]

Abstract

Throughout Covid-19, Cardiff University have adopted a blending learning solution to tackle the need for continued higher education, without risking the health of the students or staff. To combat this, most of the learning has been adapted to online learning. A problem that has arisen from this is a lack of e-leaning tools to help support students during the transition. My proposed solution was to make an educational animation to demonstrate how Diffie-Hellman Key exchange works. Diffie-Hellman key exchange is a cryptography technique learnt in the optional final year module, Security. There are already solutions like this online, however many of these are in picture or text formats and do not show the key exchange in an animation format. My product is tailored to the specific material being learnt in the module. An agile methodology was followed to produce this tool and it was implemented using HTML, CSS and Animie.js. Most aims that were set out in the initial plan were fully realised and created, with the exception of the retention study. Overall, this project is viewed as successful and able to be implemented in the available e-learning tool set come next year. This paper will display the process that was used to develop this tool, and will provide the overall reflection on the successes and downfalls of the projects.

Acknowledgments

I would like to use this section to thank Dr. George Theodorakopoulos for the support me throughout this project. In addition, I would like to thank the ethics committee for taking their time to review and process my application. My greatest gratitude goes towards the volunteers that participated during the prototype feedback and user testing who took time out of their day to view and critically analyse my project. This feedback greatly helped the development of my project. Finally, I would like to thank my family and friends which have supported me through this process.

Table of Contents

Table of Figures

1.Introduction

Online learning has seen a huge growth within the last decade, and in particular during the Pandemic of Covid-19. Throughout the pandemic, schools have not been able to perform in person learning due to the risk of the students and teacher's health, driving the need for new online learning resources and tools to help provide sufficient education. Companies and schools have had to react quickly in these circumstances and therefore have invested funding into their online learning resources and software's. The threat of the pandemic does not have a definitive end date; therefore, it is hard to tell when normal in person learning will resume again. Recently an investor, Benesse Holdings, has put "$50 million"[1] into an online learning platform called Udemy, predicting a gross profit of $2 billion due to the high usage of the site under the current circumstances that place a high demand on online learning. There is clearly a big market for more e-learning tools and an immediate need for them. When it comes to learning new information and understanding concepts, there are three schools of thought about how learning is categorised. This is: visual learning, auditory learning and kinaesthetic learning. Visual learning can be defined by "those that need to see pictures and graphs to visualize." Auditory learning is "those who need to hear the information" and kinaesthetic learning is "those who need to engage in an activity in order to grasp a concept.". [2]

In the final year of the BSc degree in Computer Science at Cardiff University there is an optional module called "Security" which "provides students with basic understanding of cryptographic tools and techniques that are used in modern systems to achieve security objectives, such as confidentiality, integrity, and authentication."[3] During this module, students learn the content through a mix of auditory learning from live lectures and visual learning through a PowerPoint presentation. In this individual project the intention was to take this content and make a security animation that will benefit visual and kinaesthetic learners as a majority of the module is taught audibly. Visual learning "increases retention by 29-42%"[4] meaning that these animations hold the potential to benefit the student studying security, allowing an interactive platform whereby the individual can understand the concepts they learn with a more visual and hands-on approach. The end goal of the project is to increase the retention rate of material, thus help the student with their exam and application of this material.

1.1 Aims of the project

The project aim was to create a security animation of Diffie-Hellman Key Exchange (DHKE). This topic is taught in the third-year module 'Security'. In this project, two animations were implemented which demonstrate Diffie-Hellman. The first is a colour mixing example, which is a common high-level way of explaining Diffie-Hellman without going into detail about the underlying maths. The goal of Diffie Hellman is for two users to create a secure channel which they can send encrypted messages without any external parties listening in to their conversation. Typically, a man in the middle attack can allow an attacker to listen in to a conversation, but with Diffie Hellman the users manage to send a message without sharing

their private keys (see Background). The second example incorporates the mathematics behind Diffie Hellman and how it secures the message using different operations. This will serve as a more advanced way of looking at Diffie Hellman, accurately reflecting the methodology required in the third-year module ‘Security.

Another aim was to create a user-friendly graphical user interface (GUI), to encase the animation that is deployed online, allowing it to be accessible to all student studying the security module. The GUI includes play and pause button functionality and navigation to the man in the middle attack page. In conjunction to this animation implementation, a further aim was to research into human computer interaction. This would allow exploration of the best way of implementing the animation and GUI so that it is intuitive and user friendly, but also creates an environment that is conducive to retain the information the users are learning. This was aided by the reading and application of external open-source materials which studied the effects of animations on learning and extracting the helpful techniques that can be applied to the animation.

1.2 Audience and Scope

The audience for this project is third/fourth year students that are taking the optional module of ‘Security’. The project that is being developed aligns with the necessary objective and learning outcomes of DHKE within this module, therefore making this animation a useful learning and revision tool. This animation will be best suited to students who identify themselves as visual/ Kinaesthetic learners. “Language teachers and researchers have recently been cognizant of the fact that vocabulary is an important aspect of language, which is worth investigating. However, learners usually admit that they experience considerable difficulty with vocabulary, and many of them identify the acquisition of vocabulary as their greatest source of problems. The problem is to discover which ways or skills will best help learners better learn, retain and retrieve vocabulary.”[5] This animation aims to provide a solution to this problem and help the students that struggle with retaining the information taught in lectures.

The scope of the project was based around the deliverables that were set within the initial project plan. These include the design, prototype and the final implementation. The design was created using a wireframe tool called balsamiq. This tool helped me see how the animation will look when implemented into the GUI and enabled me to story board the user experience without having to implement the animation. From this design a short prototype was produced using PowerPoint to animate the static images. The prototype showed the colour mixing animation and the mathematical animation, however, did not incorporate the GUI as the intention of this prototype was to understand the flow of the animations. Once the users viewed the prototype a questionnaire was given to computer science students to gather their thoughts and feedbacks on the animations. From this the useful features and the drawbacks were identified. When implementing the animation, Animie.js, HTML and CSS was used to create

the GUI and the animation. The final aim was to deploy the final product onto a public server where the students can easily access and interact with the animations.

1.3 Approach and assumptions

1.3.1 Use of Agile methodology and subsequent tools used

An agile methodology was followed while creating this project. Through every step of the development, an assessment and review of the choices made was completed with the help of feedback from current third year students and my supervisor. This helped the development and betterment of my project. This feedback was then used to edit and improve the pervious section of the development. In the agile methodology there are 6 steps which are placed in a cyclecar loop. These steps are plan, Design, Develop, Test, Release and feedback. Two tools were used to help track the time management and progress of the project.

To help me with planning, throughout the process a Gaunt chart was created (see appendix 1) which shows the time frame for each section of the development of this project and breaks down the different goals and objectives. In addition to this, the toll Microsoft Teams Tasks (see appendix 2) was utilised to help identify the progression of different tasks. This was separated into ‘To do’, ‘Doing’, ‘Finalising’ and ‘Done’. The weekly tasks and objectives from the gaunt chart and the initial report were duplicated and laid out into manageable tasks within this tool. Each time progress was made within the project the respective task would be moved over to the according section to help keep track of what stage the project was at. The wireframe tool balsamiq was used to design the animations and create a prototype which was tested with users to see what feedback they have and if anything needs to be altered. This reset the loop, again allowing the feedback to feed through the updated design of the animation. The loop structure means that if there was any need to go back and change an idea, changes could easily be made instead of having to go through the whole process before being able to alter the issue.

1.3.2 Assumptions made

The assumptions going into this project was that the animation that will be created will be targeted towards students with an underlying knowledge of cryptography (previously learnt in ‘Maths for computer science’ module) and will have a proficient background in mathematics. This is assumed as the criteria to study Computer Science at Cardiff University is to have achieved at least a A/B in GCSE, and many students have also gained A-level in mathematics. In addition to this, all students would have studied the compulsory first year module of maths for computer science. Another assumption is that students will not have completed learning about DHKE, however, will have been provided with key information of this cryptography technique during their security module. I will be carrying through the assumption that the student will be in their third/fourth year of studying computer science at Cardiff university as this is my targeted audience. Furthermore, it was assumed that as all the learning is currently online, all students will have internet access and the necessary hardware and devices required for the content and if not, then the resources will be provided by Cardiff University.

1.4 Summary of Outcomes

The key aim of this project was to produce a product that clearly and effectively teaches final year students the basic theory behind DHKE and that this tool has a user-friendly and intuitive design. A further outcome that was of a high priority was that the animation could be effectively used through the years to help students better understand the DHKE basic principles and methodology.

2. The Background

2.1 The wider context of the project

2.1.1 What is Diffie-Hellman Key exchange?

DHKE was Proposed in 1976 by Whitfield Diffie and Martin Hellman. “Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. DHKE method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.”[6] The goal of DHKE is for both parties to compute the same number K (key) and for this to be secure so nobody else can intercept the message.

DHKE is not always secure and can be susceptible to man in the middle attacks and interception via the discrete logarithm problem. An actor can perform a man in the middle attack by making Alice and Bob believe they have shared their secret key each other where in actuality it has been intercepted by Eve. Eve will not be able to see the message, but she will be able to block the correct message from being sent to Alice and Bob. She does this by replacing the intended key with her own key and performing her own exchange with Alice and Bob to create secure channels with both of them. Once she has created the secure channel, she can steal information which is sent through the secure channel.

All of the content that will be replicated in the animations is covered in the third-year module ‘Security’. This is where I learnt the information and applied knowledge about DHKE. During the process of creating the narration and content, the module slides and past exam questions were used to tailor the animation to the necessary content. To make sure that the content was relevant and useful all the examinable material from the module was included. The animation will hopefully help future students as a learning and revision aid for years to come.

2.1.2 Case Studies and Literary Research

Case studies and research papers were used to obtain background research for how to successfully animate e-learning content and the best way to make animations as learning tools. One I found particularly insightful was a study by Jean-Michel Boucheix, Richard K. Lowe. The case study focused on “An eye tracking comparison of external pointing cues and internal continuous cues in learning with complex animations” [7]. In this study, they used a group of students who had “little or no knowledge of a piano’s internal mechanism” and showed them an animation of how the piano works internally with visual aids of instructions and a visual representation. After watching the animation, they were asked to replicate what they saw on a clear glass-topped piano table. The study was used to measure “The quality of the mental model constructed as a result of viewing the animation (in terms of how accurate, comprehensive, and

appropriate it is) will determine its utility for performing specific cognitive tasks. If the externally presented material depicts content beyond the familiar and every day, it is unlikely that non-specialists will be able to generate a high-quality mental model without additional support."

"Schnotz and Lowe (2008) have distinguished two major contributors to the relative perceptibility of entities that make up an animation. One is visuospatial contrast, that is, if an entity is relatively large, brightly coloured, unusually shaped, and centrally placed, it is likely to be more readily perceived than its less distinctive neighbours." This knowledge helped guide the design for my animation. From this the conclusion was made that the animation containers should be on the same page and symmetrical, therefore the participants focus can be distributed fairly between each of the animations. To reflect the lessons learnt in this study the animation was designed so it had a clear beginning with a plain text instruction to not give bias to what the participant would click. The Text was simply instructional and used to help navigate the participant to the necessary animation. The second major contribution Schnotz and Lowe found is called "dynamic contrast" and how "the perceptibility of a specific entity may be enhanced if it is moving or changing over time in a manner that contrasts greatly with the behaviour of entities in its neighbourhood (Lowe, 2005)." A lesson that was taken took from this study was to make the page layout have multiple moving parts to make the static page more dynamic and interesting. To make the moving parts to be not distracting, the moment was only subtle and easy to follow. This would mean that the users main focused would be on informant details on the page and not the movement. An example of this is how the intro text moves slowly up and down which is reminiscing of early 8-bit games where they would have the start buttons hovering and flashing on the screen e.g., Pac Man, Space invaders, Mario. (see figure 1)

Figure 1-Design based on space invaders caption

This study additionally covers the importance of queuing the audience/learner. Figure 2 below displays the utilisation of arrows to queue the participant of where they should be focusing for certain parts of the animation. "For information extraction to be effective, it is crucial that learner attention be directed to precisely the right locations in the animation at precisely the right times (Lowe, 2008)." In my animation two different columns were used to hold Bob and Alice so the user can clearly see the location of the keys at each part of the key exchange.

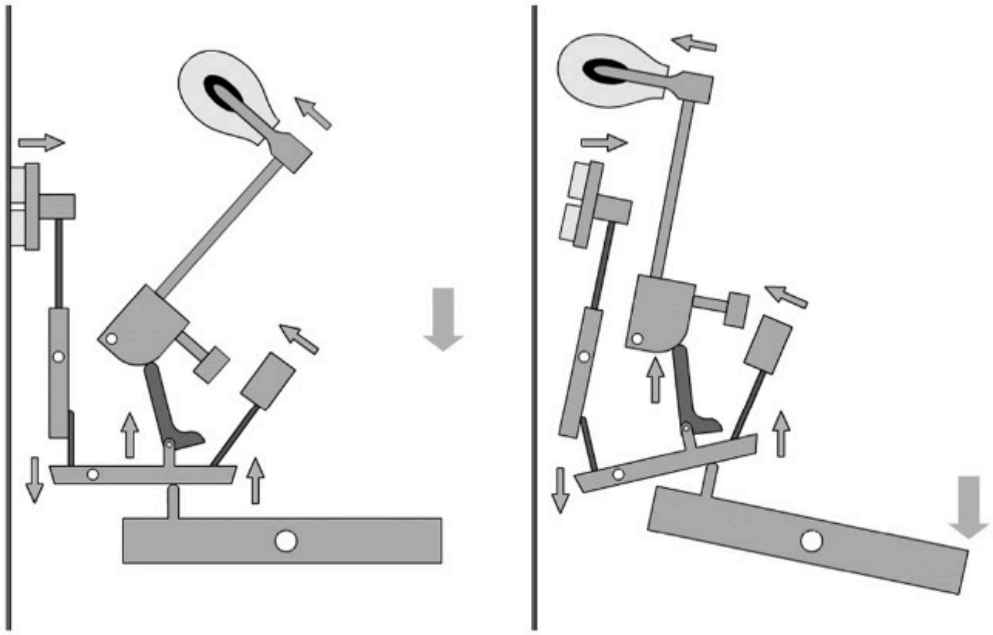


Fig. 1. Piano system with arrows indicating movement of parts.

Figure 2- cueing animation

2.1.3 Generating vs. receiving instructional explanations Case study

Another study that influenced the design and furthered the understanding of the psychology behind learning was created by Björn B. de Koning*, Huib K. Tabbers, Remy M.J.P. Rikers, Fred Paas. This paper investigated 'generating vs. receiving instructional explanations: Two approaches to enhance attention cueing in animations' "This study investigated whether learners construct more accurate mental representations from animations when instructional explanations are provided via narration than when learners attempt to infer functional relations from the animation through self-explaining."

This study is similar to the aims and outcomes that my project aimed to achieve. After the students have viewed the animations, the hope is that the students will be able to apply the learnt knowledge to an examined test. This study helped the understanding of the functionality needed to make this learning tool as helpful as possible. An example of how this study influenced the animation was that the study found that "highlighting a subsystem at the moment that the information in the narration explains the functioning of that specific part of the animation may encourage learners to make a connection between corresponding elements in the two representations." Therefore, additional text was added at the bottom of each animation narrating what was happening in the Key exchange at every step of the process.

This study also explained how "Lowe (1999) demonstrated that novice learners have difficulties in the identification and subsequent processing of relevant elements in animations,

because their attention is often diverted by superficial features such as bright colours and fast movements that are not necessarily relevant for understanding the content."[8] To discourage from having this issue occur with the animation, a focus was put on the relevant and important elements over just making the animation visually appealing. When creating the animation, it was ensured that the animation was going at a speed that is appropriate for new learners of DHKE. A singular colour pallet was applied to the design, so the visuals are not too overwhelming and distracting to the user.

2.2 The problem that has been identified and stakeholders involved.

During Covid-19, Cardiff University moved the majority of lectures and learning online instead of the traditional in person lectures. This transformation started in March 2020 and has continued to present day. This means that all the resources that student are receiving have been reduced, as students would have had the opportunity to have a more personable experience with their lecturers and learning. Face-to-face learning gives students the "ability to discuss, collaborate, practice and role play, all 'live' and with guidance from a facilitator on hand. Being part of a group and being held accountable are powerful learning tools."[9] Frontiers in computer science did a study of "A Comparative Analysis of Student Performance in an Online vs. Face-to-Face Environmental Science Course From 2009 to 2016" This study found that there was 'no significant difference in student performance between online and face-to-face learners'[10], however, when I conducted a poll with third year students about what they enjoyed more online learning or face-to-face learning I found that 70% preferred online learning, with 100% of the women who voted enjoyed face-to-face learning better. There are many components that may have biased this decision as the face-to-face learning was during their first and second years which are seen as more enjoyable then third year, making this poll not objective. Nonetheless, there was an overwhelming opinion that the face-to-face learning is better than online learning.

In my opinion, the encouragement of participation and involvement which face-to-face teaching allows students to have has not been successfully duplicated for the online learning. Therefore, it's important that the university has more interactive and visual tools that can engage students more in the content they are learning.

The main stakeholder for this animation is third/fourth year BSc students who have chosen the optional security module. Within this module they learn about "basic understanding of cryptographic tools and techniques that are used in modern systems to achieve security objectives, such as confidentiality, integrity, and authentication. Students are introduced to relevant practical aspects as well as to the mathematical foundations of these techniques. Finally, the module goes into real-world security protocols (such as SSL/TLS) and how they are composed as a combination of basic techniques." [11] One of the lectures covers DHKE and the advantages and disadvantages of this cryptographic technique. Students will then apply this knowledge to an exam. In 2020, the module content was split into three individual exams which were worth 33% (the final exam being worth 34%). DHKE is taught in the second section of the module and is tested in the class test #2. This animation aid can be used by students to help them better understand the theory of DHKE exchange from a high- and low-level point of view.

This animation can then be used again to help students revise for the in-class test as it provides similar examples to the type of questions they will be tested on in the exam.

Another stakeholder is the School of computer science and the lecturers teaching this module. This animation will be provided to both stakeholders for them to show during their lectures and provide to the students as an additional resource. This will benefit the lecturer as it gives them another platform for interactivity for students, which could improve student satisfaction as they are being provided more tailored resources. Higher student satisfaction will help the university during the National Student Survey (NSS) which each student takes at the end of each academic year. This survey then impacts the university's score on the league tables. The university wants to be as high as possible on the league table as this is a reflection of how well the university is doing academically and the student satisfaction. The higher the university is on a league table the more likely students are going to want to study at that university therefore resulting in more income for the university.

2.3 Theory associated with Diffie-Hellman Key Exchange

To set up DHKE, two parties (Alice and Bob) both choose and agree upon a large prime, *p,* and a primitive root, *g* of *p*. Finally they will publish *p,g.*

Step one of DHKE is for Alice and Bob to generate their individual private keys a,b which they will never share. Alice will compute g^a mod p creating her shared key A. Likewise, Bob will compute g^b mod p creating his shared key B. Alice and Bob will then send each other their shared keys. Note that 'even if the traffic is recorded and later analysed, there's absolutely no way to figure out what the key was, even though the exchanges that created it may have been visible.'[12] Once Bob and Alice have received each other's shared keys they will then repeated the same operation but instead of using G they will use the shared public key. Alice will compute B^a mod p and Bob will compute A^b mod p. Once this is computed Alice and Bob will be left with the same Shared key K.

Because Alice and Bob don't share their private key, it reduces the risk of a third-party attacker (Eve) from intercepting the message. At the end of DHKE Alice and Bob know $k=g^{ab}$ mod p and all Eve can know is *p, g,* g^a *mod p,* g^b *mod p.* This is not enough to compute g^{AB} *mod p,* unless Eve computes the discrete logarithm *of* g^A *mod p or* g^B *mod p* to find either *A or B.* DHKE is particularly useful because anyone analysing the traffic at a later date cannot break in because the key was never saved, never transmitted, and never made visible anywhere.

2.4 Constraints on the approach to be adopted

The animation is hosted on a website and will only be accessible with WIFI and via a web browser. The user needs the URL to view the animation. The source code is also posted on GitHub which means students can download then run locally if they want to view the animation offline, however, internet access would be required to download the source code initially. Another constraint of the animation is that the design of the animation is for devices such as a

laptop or computer and will not be adapted to scale for a phone or tablet. The animation will also not be made into an app or be accessible outside of a web browser.

The animation is static and does not include any user input to affect the animation. Therefore, there is no user interaction with the animation e.g., inputting the values to be used in the maths example. In addition to this the animation only included an example for each of the animation, therefore they will only see the example with one set of numbers and will not get to see how other numbers will affect the result. This also applies to the colour mixing example and both man in the middle attack examples.

Some learning tools at the end have a quiz or a test so see if the user has understood and retained what they just learnt. In the animation this is not included but is a future goal to achieve and will be added at a later date.

2.5 Existing solutions

2.5.1 Videos

When researching existing DHKE animated tools for e-learning, I was not able to find any live animations hosted on a web page which is similar to my design and implementation. However, there is a lot of accessible content on Diffie-Hellman online in many different formats. The most similar format to the animation is videos explaining the DHKE. These videos typically have a short introduction to DHKE then show how Alice and Bob generate and exchange their keys to get a matching shared key at the end. Most of these videos also explain DHKE using the colour mixing example, which is the same example that the animation adopts. However, disadvantages of these videos are they can be long and not very concise. The top ten results in videos for DHKE (from google) ranges from time from 2:19 minutes to 34:11 minutes and average at a time of 11:19 minutes. These videos are also not specific to the content that is taught in the security module, whereas my animations are tailored to the content that students will be using in the module. This means that students will not need to be watching long videos that have non-exanimate content. An advantage of these videos is that they have audio accompanying the visual aspects of the explanation. This means that it is accessible to visual and auditory learners. This may be something that might be worth considering adding to the animation in the future.

2.5.2 Online DHKE generators

Another existing solution that is open source is Diffie-Hellman generators online. These generators ask for user input of numbers and output Alice and Bobs keys that they generate thought-out the process and finally return the shared key solution at the end. This is beneficial as it is more interactive with the user and allows them to test out their own numbers and see how it effects the output. The generator also has options for the user to make the website generate the required numbers instead of the user manually inputting them.[13] However, this solution is a learning tool. The generator does not have explanations of what is happening with

the key exchanges and so on. The DHKE animation has specific text at each point of the process explaining what is happening and why a particular solution has occurred. In addition to this, just generating a solution can be used as a tool to help students cheat on a test because is they are not applying their knowledge and just plugging in the required numbers and not applying their knowledge. In the future, extra functionality may be added to the animation where users can input their own numbers and observe how this will impact the output and security of DHKE. However, like stated above there is the concern that this will make students less likely to understand the theory behind DHKE and use the animation as a tool to get solutions.

2.5.3 Images

The final common solution which is similar to the DHKE animation being produced are images which display how the key exchange works. These images are static and display the process of DHKE. There is a wide variety of examples and images online which are a helpful resource to students who can select the image or example that works best for them. The animation in this project only has two examples: a maths example and a colour mixing example, and even though these are the most relevant and common examples some students might not like how they explain DHKE. This solution has highlighted that there might be a need to add in more ways of demonstrating DHKE in future updates. The images also have a variety of difficulty and complexity which could also be incorporated into future iterations of the animation. The animation being produced has one high level and one low level example in my solution, but it might be useful for students to be able to select the difficulty before starting the animation so they can slowly build up their knowledge, instead of having only two options which are not clear how advanced they are.

The DHKE animation is not made to replace any of these above solutions, but instead to extend and complement the open-source information found online. This solution will hopefully give more tailored examples for the security module. Students can use the animation in conjunction to these online solutions and use them as background research which may give more context being DHKE which is not covered in the module. Past paper questions that were used as examinable material is the module have been used to help create the content in the animation to make sure all relevant information has been inputted into the animation. For example, one of the exam questions is to order/show the stages of DHKE events and this this what is shown in detail in my animation. (see appendix 7) The animation also breaks down the mathematical equations and solutions for DHKE which will help with the more applied questions which involve calculating a solution.

2.6 Methods and tools used

To design the animation and GUI, a tool called balsamiq was used. Balsamiq is a drag and drop wireframe tool that allows designers to experiment with different layouts and features. This was ideal for the animation as it allowed for a structured creative design which reflects industry standard designs. Balsamiq also lets you import and draw your own which allowed me to put

my own unique style on the design. This tool boasts the options of many platforms to design the application on such as iOS, android, search engines etc.

An agile methodology was adopted throughout the process of designing, implementing and testing the animation. I planned to perform user testing throughout the whole process of developing and implementing the animation and let the feedback determine and aid the changes that I made for the application. The initial designs were tested on current third year students who already have a background knowledge of DHKE. This allows them to give more comprehensive feedback that a novice may not have. User testing was again used after the first build of the animation which gave important feedback and suggestions which were fed back into the design and implementation of the animation. Good user testing produced a better understanding of the strengths and weaknesses of the animation and GUI.

Other tools that were used throughout this process were the IDE atom to code my application. HTML, CSS and JavaScript were used to implement the animation. The JavaScript library that was used was called animie.js. This is a is a lightweight JavaScript animation library with a simple, yet powerful API. In addition, the animation is hosted on GitHub pages allowing the students to have an online version of the animation, but this also gives them the option to download the source code if they want to run it locally.

2.7 Background reflection

The aim of the project was to resolve the issue that there are not enough tools to help visual leaners understand the concepts that we study in the modules at Cardiff University. This was identified through the background research of existing solutions and how there are currently no open source DHKE animations. This project endeavoured to solve this by making a custom animation detailing the stages and theory behind DHKE which will be available to all third years who chose the optional module of security. In order to develop a strategy going forward, key stakeholders were identified and their requirements for the tool were applied. The lessons learnt from the case studies helped identify what requirements aims should be applied to the project. This animation will help students visualise how the key exchange works and what happened if a man in the middle attack occurs. Currently in the module this is taught via static pictures and auditory explanation by the lecturer. The goal of this project was to see an improvement in the students understanding and retention on this topic and help them improve their mark in a test that covers this topic.

3. Specification & Design

3.1 Business Model:

The business model of the application is a ‘Online educational business model’ as the main clients of this project are university students who want to learn about DHKE. This product is free to users and the source code is open allowing the students to have the option to download and alter the project. A vertically integrated supply chain has been used as I managed, designed, implemented and distributed this product.

3.1.1 User and Business Requirement

To help define the user requirements user stories were created. (see figure 3 and 4) This was produced to get an idea of the kind of users who would use the animation and envision the key goals the user would have and the challenges they currently face.

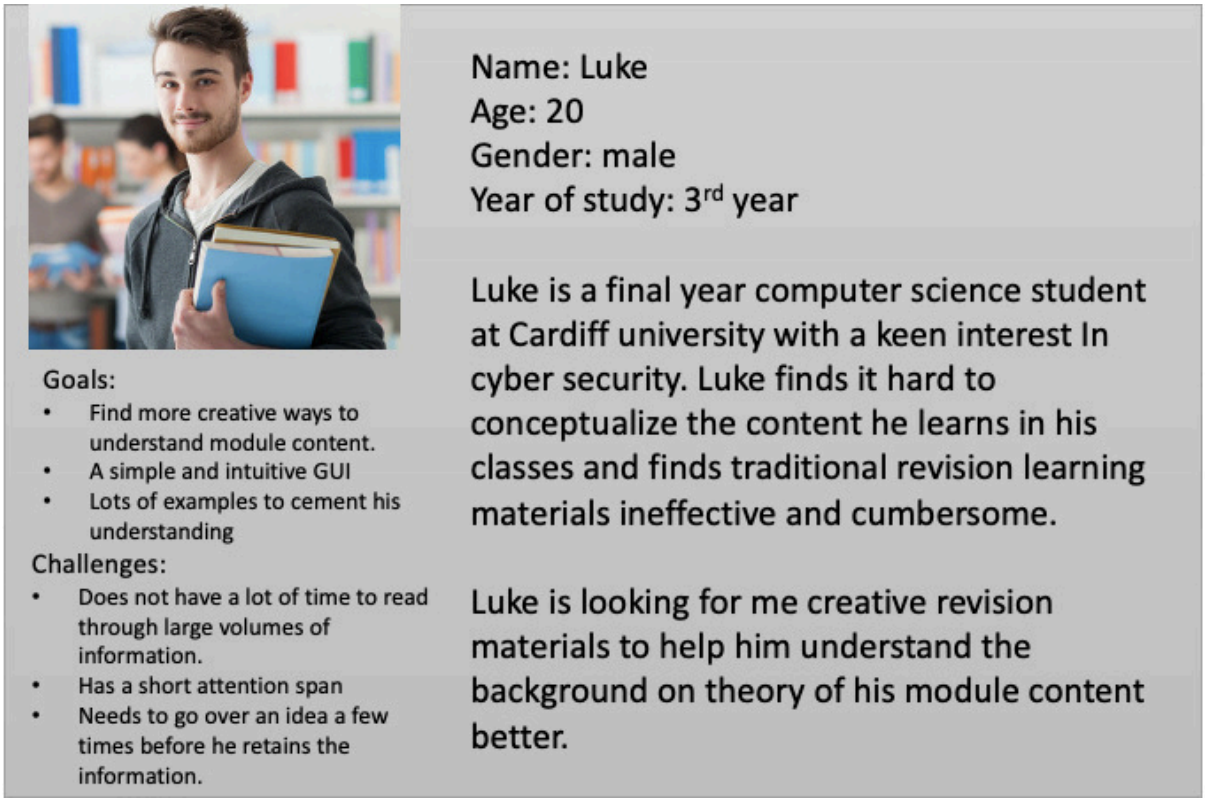


Figure 3- User story: Luke

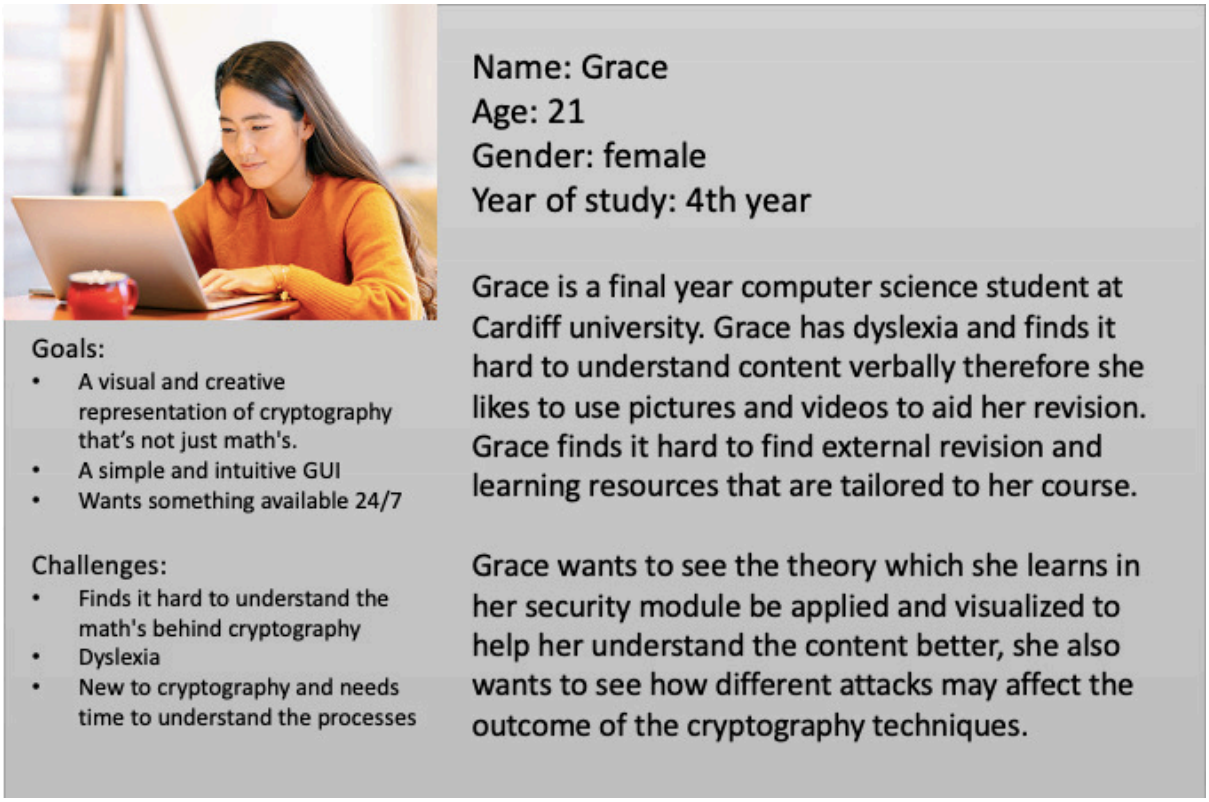


Figure 4-User story: Grace

3.1.2 User requirements

From the user story requirements were created this helped inform the design and implementation of the animation:

1. Create a DHKE animation with clear explanation and detail on the process of the key exchange.
2. Create two animations one that can show the more mathematical and advanced example of DHKE and one example which shows DHKE from a metaphorical example (colour mixing example)
3. Create a visual animation which does not include a vast amount of text
4. Create a simple and intuitive GUI
5. Include content in the animation which is relevant to the security module content.
6. Create an animation which is at a speed conducive to learning.
7. Users Have the ability to replay/re-watch an animation

3.2 Designing the User interface

3.2.1 Overview of the final design

Figure 5 displays the final designs used to influence and create the implementation. The first page is 'home' page of the DHKE animation. This is the first page users will see when opening up the URL. The design of the home page consists of two container boxes which is where the animation plays with in. One box holds the maths example and the other holds the colour mixing example. There are clear start and stop buttons underneath the design which trigger the animation to play and pause. At the top of the page there is a heading which clearly identifies what page the user is on. The maths example consists of mathematical equations which show how each key is created, this is accompanied with narration at the bottom of the box. The colour mixing used colours instead of the equations to symbolise the keys being created.

The next design is for the man in the middle attack page this follow the same structure as the home page however incorporates the arrival of an attacker called Eve. Eve has her own column in the box meaning that the container in the DHKE man in the middle page is bigger than the home page containers. Another change to the container is that the background colour is a light red instead of white. Eve is represented using a name text identifier and the use of the devil emoji.

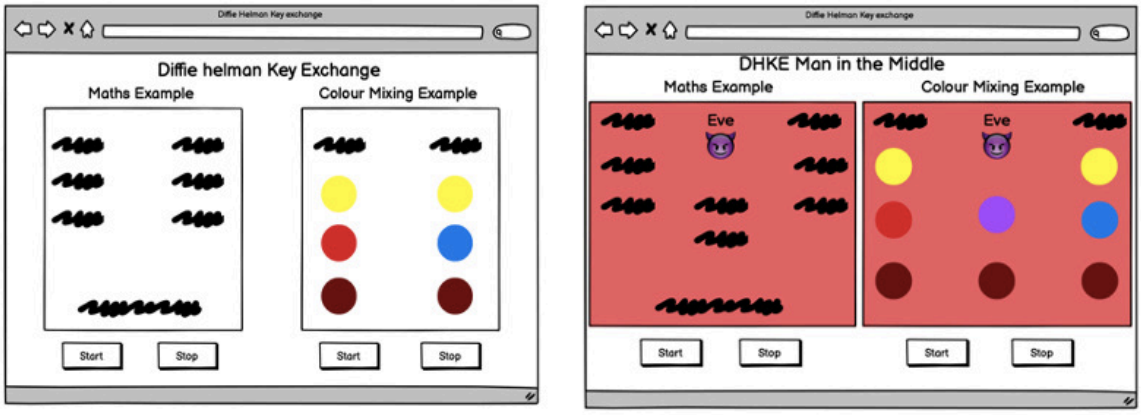


Figure 5-Final GUI designs

3.2.2 The design process

The first thing that was produced before designing the interface was a small diagram with the necessary functionality that needs to be included in the design. This enabled a clear idea of what needed to be included and where. (see figure 6)

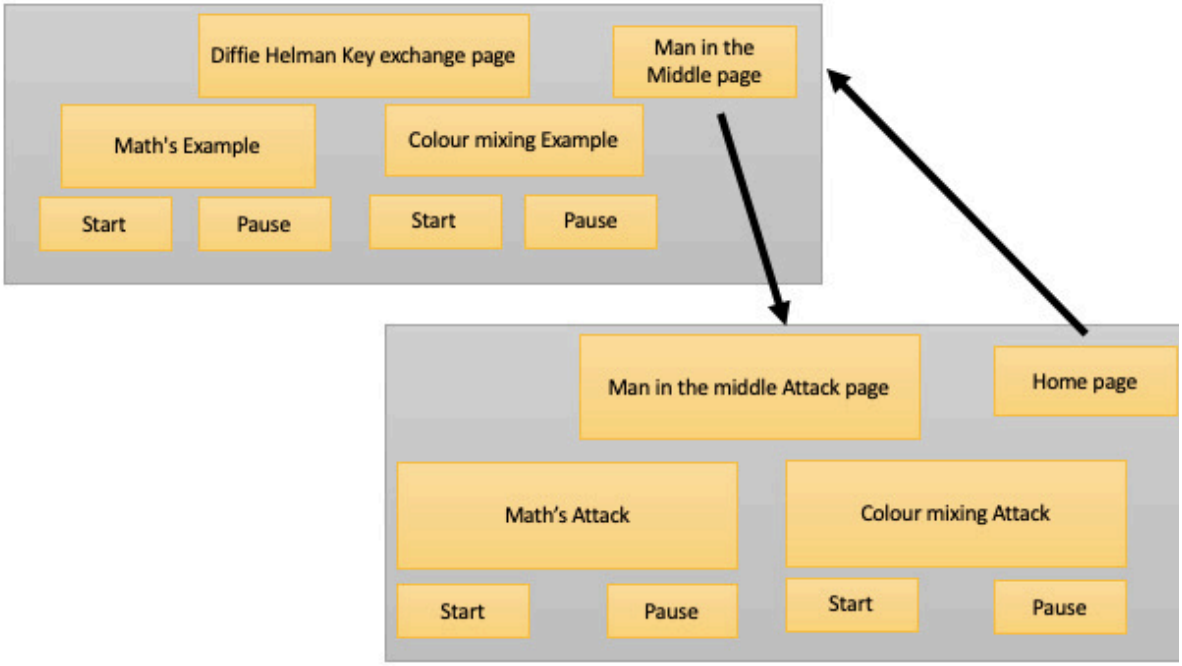


Figure 6-Flow of design

When designing the first iteration of the GUI, the intention was to put both animations to fit onto one page. This was so the user could easily compare the two animations and understand the similarities between both of them. Balsamiq was used to create the wireframes of the User Interface for the basic animations. Figure 7 below displays the first attempt for the static design of the animation. The goal was to make the animations as simple and effective as possible to fit the user requirements of having a 'simple and intuitive GUI'. On the left is the colour mixing example, which follows an online image example that was found while researching about DHKE (see appendix 3). This image was used to inspire the colour scheme utilised and how the colour mixing idea is portrayed. The difference between the image and the animation that I will be producing is that animation will be dynamic, unlike the static image online. On the right of the figure 7 is the design of the maths example. This design includes a more textual and mathematical based example with the words moving around the box instead of the coloured circles. In the constraints adopted have no user interaction or input, so the only inputs that the user does is the use of the start and stop buttons for each of the animations.

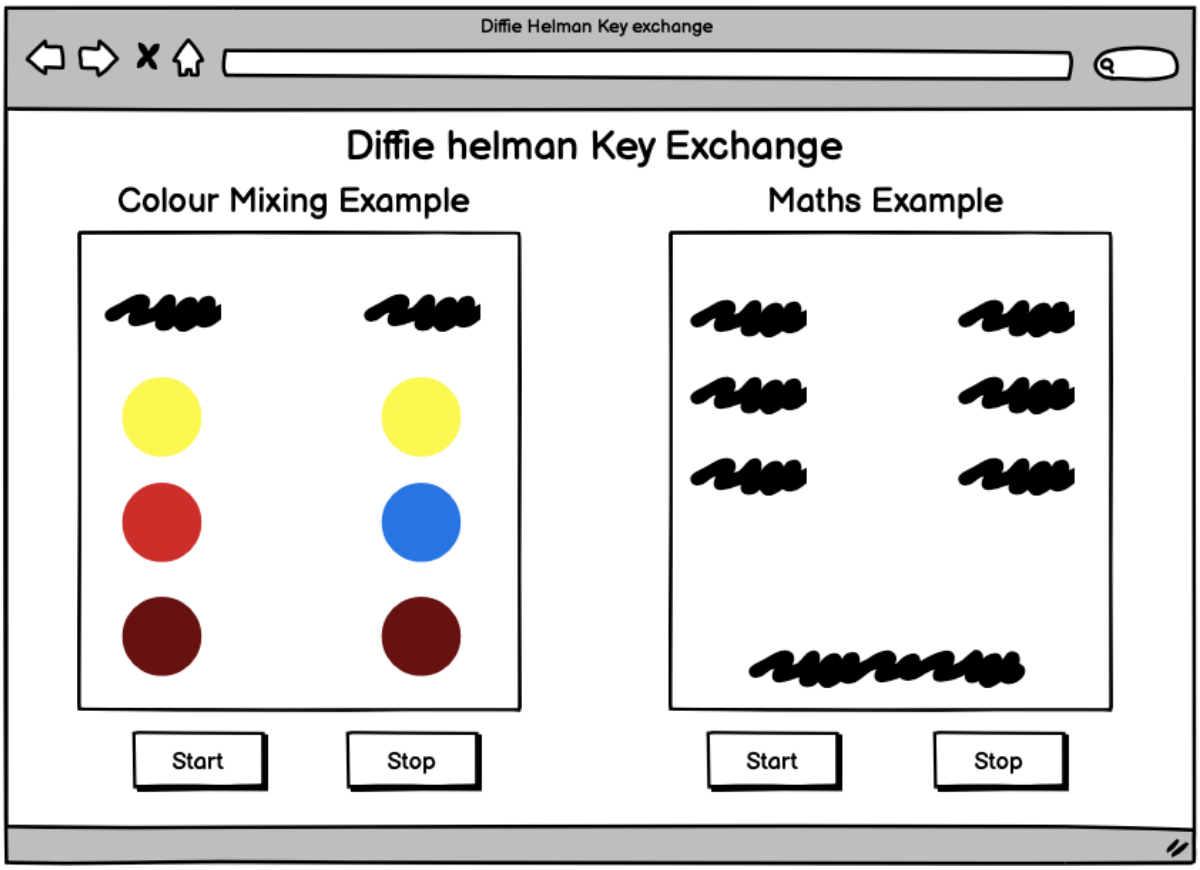


Figure 7-colour mixing design 1

3.3 The dynamic behaviour of the system

3.3.1 Creating the prototype

After the basic wireframe static version was designed, the next step was to prototype the design with the elements moving around the page to gain a better idea of the flow of the animations and how the objects will interact with each other. The prototype was made using PowerPoint as it has animated feature which have inbuilt animations, in turn making it simple to test different movements and interactions. When creating the prototype, the decision was made to change the circles of colour to pain splats as this would visually look more appealing to the user. Narrative text was added at the side of the animation that would describe what was currently happening. This was included to reflect conclusions made in the 'Generating vs. receiving instructional explanations' Case study (see background 2.1.3). The decision to add this into the project was so the animation would be more accessible to the stakeholders as most of the students would of not have learnt about DHKE exchange, therefore the animation was altered to make sure that this would be accessible for even complete beginners. However, while designing the assumption was made that users would have a basic understanding of computational mathematics as it is taught in the first year of the computer science degree at Cardiff university. An example of this is how there is no explanation of how mod operations works. The students were additionally assumed to have a basic understanding of cryptographic

techniques like public and private keys, so these are not explained in the narration either. (see 1.3.2)

The prototype (see figure 8) mimicked how the maths modular works in the colour mixing by mixing ‘P, G’, which is yellow, with Alice’s and Bobs private key (red and blue). When they are mixed together the colour of the paint splatter changes to a new colour (orange and green). Then the animation demonstrates how the keys are exchanged by moving them across the screen so allices public key would be in Bobs side of the page and vice versa. Finally, the exchanged public keys are mixed with Alice’s and Bobs private keys again crating the final colour which is brown for both of them. This is how the flow of the animation works in both of the animations, however, in the maths animation (see figure 9) the colours are replaced with text. The decision was made that moving the text across the screen was not very visually dynamic, so to combat this a key underneath each maths equation was incorporated to better visualise what was being created. The key was also coloured which aligns with the colours used in the colour mixing example. This was done with the intention that the user will then get a better understanding of how the two animations mirror each other.

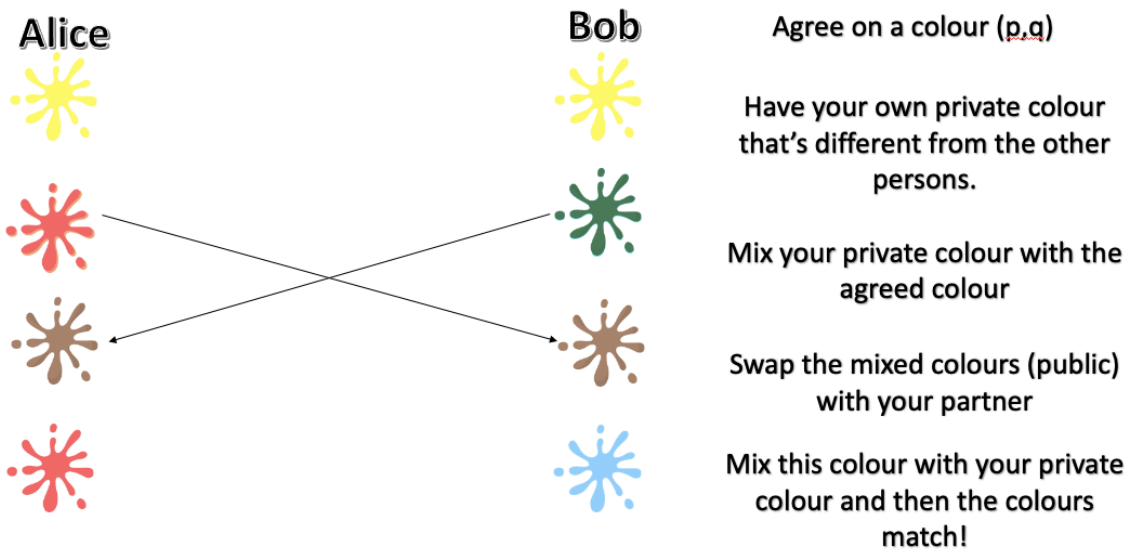


Figure 8-Colour Mixing prototype

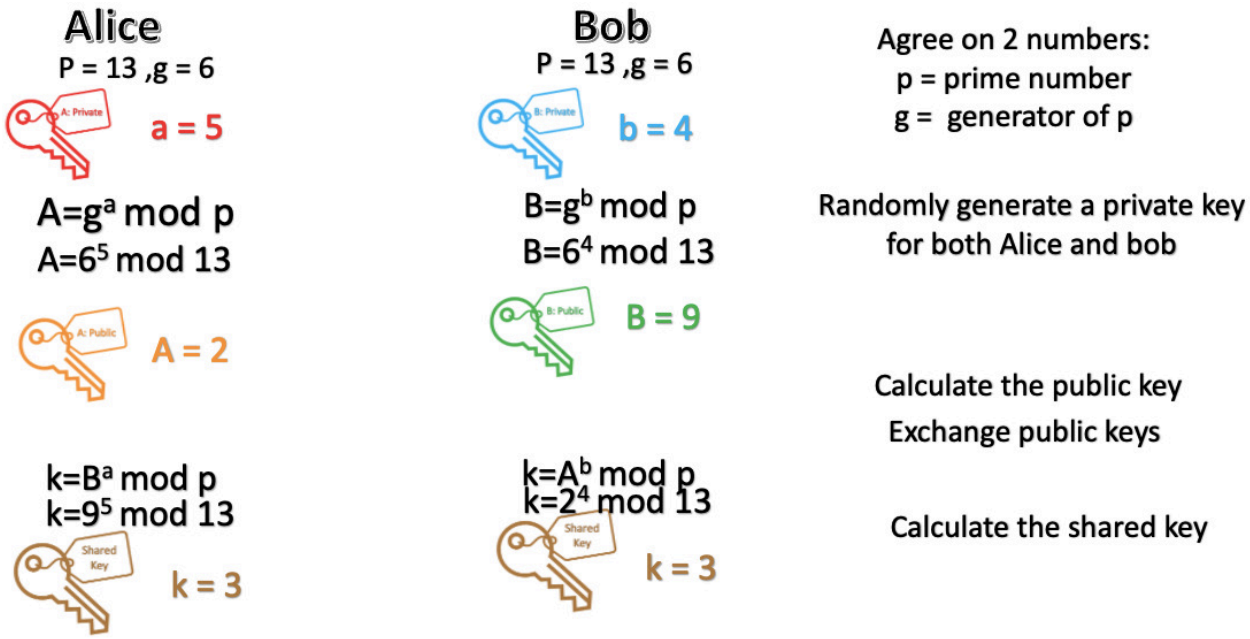


Figure 9-Maths's example prototype

3.3.2 Prototype user testing

A feedback form was created for volunteer third-year students to review. (Form in appendix 4) The protype video was sent to the volunteers with the two prototypes showing the flow of the animation and the key stages. This animation was a pre-recorded video with no interactive capabilities. In the implementation user interaction functionality such as play and pause buttons were added but this was not reflected in the prototype. This was to ensure that the basic learning was suitable before making it more complicated.

The two prototypes that were shown to the students were the colour mixing example (which gives a practical, metaphorical example of how DHKE works.) Out of the 5 participants, 40% found that the colour mixing animation was clear, 40% thought it was clear but could be improved upon to give more clarity, and 20% did not think it was clear at all. The feedback form then prompted the participants who responded with 'yes but it could be clearer' or 'no' to give an explanation of why they thought this. From these responses the conclusion was made that the lack of accompanying textual information or numbers made it hard for them to follow how the key exchange was working. These comments informed the decision that extra textual summary with the amination to make this clearer. It was also decided that it would be beneficial to show the colour mixing example after the formal key exchange example as it put the maths into a real world applied example and this may help them cement the knowledge, instead of the other way round.

The next question was if the students found the mathmatical example usefull/clear. 40% said yes and 60% said yes, but could be clearer. It is interesting that with this one, no one said no, unlike the previous animation. The biggest issue that people found was with the number

susbstitiutions into the provided equations and that this could be clearer. A suggestion was that the equations were not replaced with the plugged in numbers and instead both should remain on the screen so the user can compare them. To make it clearer where the numbers are coming from, it was sugegested that the animation could show the numbers coming from the places on the page (like a shadow duplication effect).

At the end of the questionaire overall feedback was asked to be commented on via the question "thoughts on the design of the animation and is there anything else you would add". Lots of the feedback for this question were cosmetic changes that were helpful such as implementing "Two columns differentiated by column boxes for Bob and Alice so we can see them as two different people. Then when various areas merge or switch over between the two, they can travel in the empty space areas.". These additions will hopefully make the animation clearer for the viewer. I also asked if "there any other functionality or animations that would help you better understand Diffie Hellman key exchange" most of the replies were no and that the focus should be on refining the two examples.

Finally, the users were asked to express which animation they thought was the most useful. To my surprise 60% of the students said it was the mathematical example. The expectation was that the colour mixing example, but actually no one specifically chose this one; 40% said that both together was the most helpful.

Because most of the users found that the maths example more useful than the colour mixing, the decision was made to amend the original design so that the maths example is on the left of the screen as this is the animation that a user would play first. (see figure 10) This is because in the English language, we inherently read left to right. With this amendment the hope was that the users will get a better understanding of the logic of DHKE before they can see it in a 'metaphorical' more visual way.

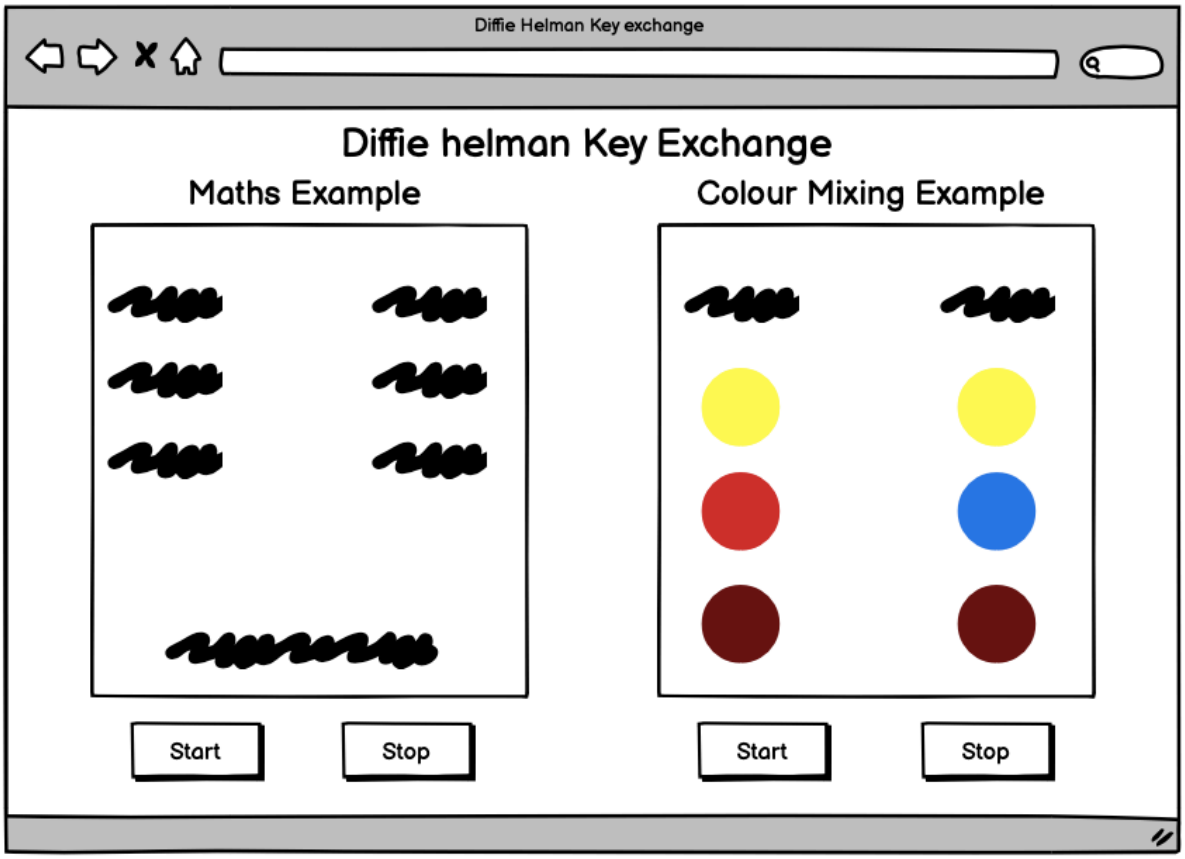


Figure 10- Updated GUI design

3.3.3 Design amendments and additions

During the implementation, the decision was made to add two additional animations. These animations would detail how a man in the middle attack would affect the maths and colour mixing example. These were added due to the fact that more time was allocated to the implementation than needed. This meant there was time to improve and expand the learning for the users. The concern was that just the two basic animations would not be enough content to help the students learn the necessary theory for the security exam. Due to the agile methodology being used throughout the project, even though the current status of the project was in the development stage, I was still able to go back to the design to create the man in the middle attack animations. The design followed a very similar layout to the basic DHKE animations but involved an extra 'actor' called Eve. Eve Is an attacker who's aim is to intercept the exchange with Bob and Alice and pretend to be each of them to create a secure channel between herself and Alice/Bob. To highlight that she was at attacker and had malicious intent an emoji was used and displayed underneath Eve's name. This was decided as it would clearly and visually represent the difference of Eve. The emoji that was chosen was the devil emoji. This devil emoji gives users connotations of evil and malice, thus utilisation of this emoji clearly identifies Eve as someone not to be trusted. Another reason for using the emoji was that the identified target audience are students who use emojis frequently to express their emotions, therefore the thought was that this would display the intent of Eve succinctly in a way that the users would understand. The awareness of Eve being malicious was additionally symbolised

by turning the background colour from white to red. Red is associate with danger and fear making it a fitting colour to use. The change of colour also differentiates these animations form the basic DHKE animations as the layouts are very similar. The worry was that the users might get the animations confused, therefore this colour change will hopefully prevent this. (see figure 11 below)

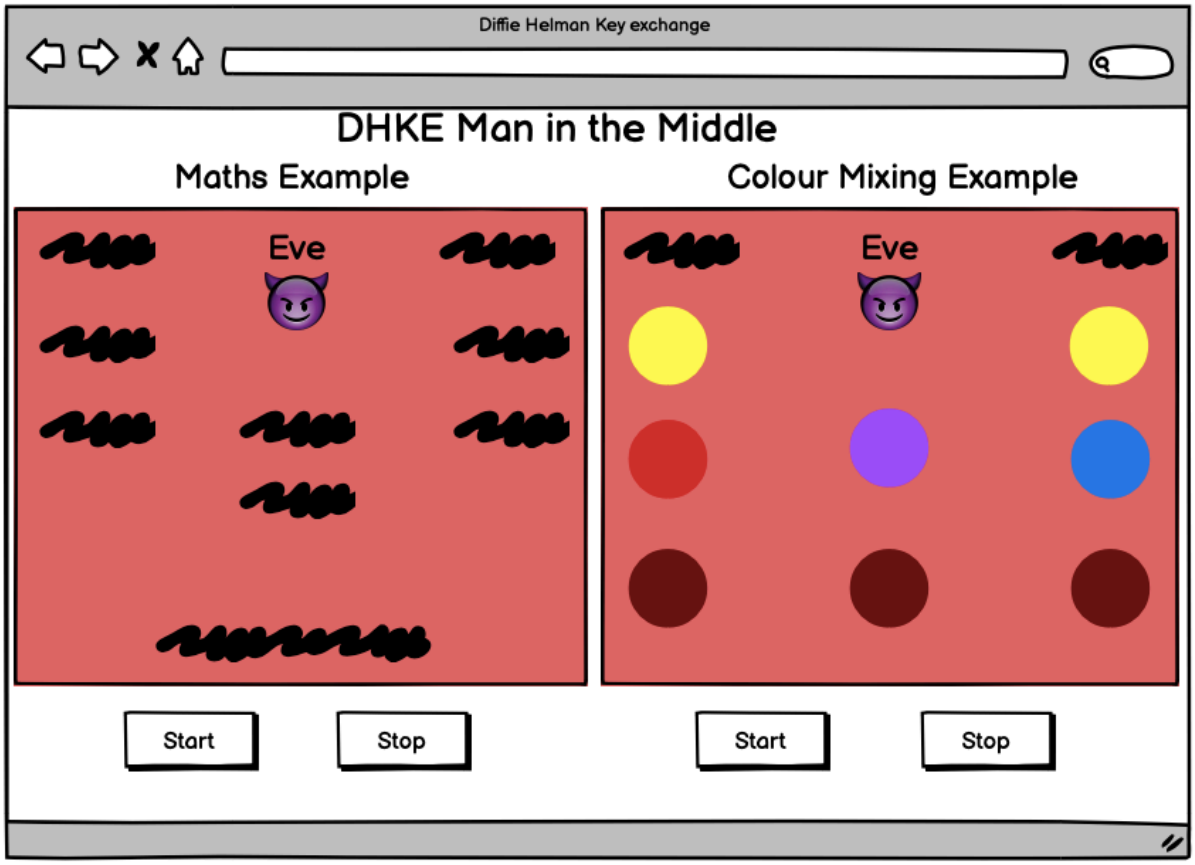


Figure 11- Man in the middle design

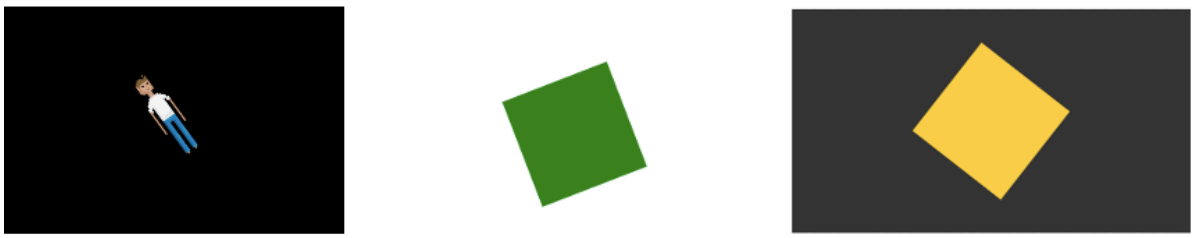
3.4 Choosing how to animate my project

To animate the DHKE the choice was made to use animie.js. At the beginning of this project, I decided to research the most popular and powerful JavaScript libraries that I would use to animate the DHKE. From this research the JavaScript libraries chosen to experiment with were animie.js, pixi.js and processing.js. To choose the language that was going to be used the decision was made to make a small animation for each of the libraries. The animation consisted of an object rotating 360°. This allowed me to get an idea of the syntax of the langue and helped the comparison between each of the languages. The first thing that was compared was the resources online for each Library. As these langue's were new to me it was important to find a language which had good documentation and examples to help me fully understand how the language works. Pixi.js and Processing.js both has documentation, but this was not every interactive and was hard to find specific examples and information. The layout of the documentation was cluttered and, personally, very confusing. Animie.js has great documentation with a very intuitive and modern webpage which demonstrates all the key

features and how they can be used for different purposes. Animie.js is also a widely used animation language so there was also a lot of external community help on sight such as stack overflow and Codepen. When animating the simple animations, it was quickly identified that processing.js was my least favourite language to use. Processing.js has a powerful API, however it required multiple setups and I found the naming conventions for some of the functions very confusing and time consuming: even the simplest functions required more work e.g., to make a rotation the language required the syntax rotate(radians(r)); and define r in a loop. In anime.js the syntax was a simple as rotate: [180, -180].

Pixi.js has some powerful features like Multi-platform Support, Interactive, visually compelling content on desktop, mobile and beyond, all reached with a single codebase to deliver transferable experiences and an Easy API. I found that this language was good for manipulating singular objects, but not as good at adding more features. Also, when looking at the comparison between all three languages, pixi.js required the most lines of code to create the rotating square. More so, pixie and processing required you to create an environment first (canvas/void) which you can see in figure 12 as the black and grey boxes in the images below. I did not like this as it restricted my animations and made it harder to integrate the animations into a GUI. Anime.js does not require this (canvas/void) making my animation more free and easier to integrate with the user interface that was being created.

Finally, animie.js was tested to create this simple animation. It was discovered that the langue was very high level and very intuitive. I liked how it easily connected with HTML and CSS objects. Just from the small animation it was evident that the language did not require a large amount of code to produce this simple animation, unlike the other libraries e.g., pixi.js. A further advantage was that the language could miniplate and incorporate SVG within the animation and because of this extra functionality. The decision was made that because of this functionality, that SVG should be incorporated into the animation. This gives it a more professional and impressive look. Overall, I felt the most comfortable using this library and decided this would be the best choice going forward with my animation.



Processing.js *animie.js* *pixi.js*

Figure 12-Comparison of JavaScript Libraries

4. The Implementation

4.1 Overview of the implementation

Four different animations were produced encompassing two different pages. These animations were a maths example, colour mixing example, man in the middle attack (maths example), man in the middle attack (colour mixing example). (see figure 13) To create the animations different timelines were made. Each page has three animations there were created, the intro animation which animated the heading and animation synopses. These were auto-play animation which started once the user navigated to the page. The animations of these objects were simple movements (see 4.2.2). The other two animations were stared by the triggering of the play button on the GUI. Both animations showed DHKE however the maths example showed this from a technical low-level viewpoint (see 4.2.2) while the colour mixing example was more metaphorical and high level (see 4.2.1).

The DHKE Man in the middle page was navigated to via a hyperlink image of the devil emoji on the home page. The implementation of the man in the middle page followed the same structure as the home page however showed use the addition of the actor Eve to demonstrate how a man in the middle attack occurs. (see 4.4) Again in this implementation there are two examples which were triggered to play via a 'play' and 'pause' button.

Figure 13-final implementation preview pages

4.2 The implementation process

4.2.1 Colour mixing example implementation

Once the initial design was amended and I was comfortable with using animie.js, the process of the implementation began. The decision was made to separate colour mixing example and the maths example. This was decided as it became apparent that it was easier to do them separately then merge them together. Once the minimal viable product (MVP) was produced the process to combining them back together began. I started with the colour mixing example as it was the simpler of the two designs and it would allow me to have more creative space to understand the new language. To be able to view the result of the code, a Python local host was used, and this was viewed via a web browser. The advantage of this was the animation could be viewed easily on the intended environment. When implementing the colour mixing example, two files were used: colour.html and stylesheet.css. The HTML file held all of the necessary HTML and the JavaScript code, while the CSS was in a separate file. When implementing the animation there were two object that were focused on: the coloured circles

and the narrative text. The decision was made to revert to my normal design of basic circles instead of the paint splatters because one user's feedback was confused about what it was, and this distracted them from the animation. Additionally, from the background research it was found that too much deign could be distracting for users. The first step of animating these objects was creating an animie.js timeline which incapsulate all of the necessary animations in order of when they should appear, disappear, and have movement. The timeline that was created for the simple colour mixing example was called basicTimeline. This timeline is triggered to start when the 'Play' button is clicked by the user and also has the ability to pause when the 'Pause' button is clicked. To make the object appear the 'easing: "easeInOutExpo"' statement was used. As well as the easing the opacity is set to 'opacity: [0,1]'. This makes the object start at 0 opacity and by the time the set duration is completed the object will be at 1 opacity. When the object to disappear, the same method is applied but in reverse; instead of the opacity being [0,1] it was changed to [1,0] so the object goes from full opacity to 0 opacity.

The first stages of the animation are P, G being published and Alice and Bob's private key appearing alongside the relevant narration. (see figure 14 screen grab 1) Once they both have appeared on the screen, the P, G colour (yellow) mixes with Alice and Bob's private key (Red, Blue). This was implemented by translating P, G down the Y axis until it was in the same pace of the private colours. The next step is the reduction of the occupancy of P, G to 0 and changed the background colour of Alice's private colour to the result of the mixing which is Orange (as yellow and red make orange). This also happened with Bob's private key making it Green (Yellow and Blue make Green). These new colours represent Alice and Bob's public keys which they then swap with each other. (see figure 14 screen grab 2) The Objects next movement needed to be diagonal to symbolise Alice and Bob exchanging their public keys. Creating this effect was initially complex as there was no obvious documentation online about how to do this. It was decided to attempt translating the X axis and the Y axis at the same time to see if this would result in a diagonal trajectory. Luckily this worked, and it was just a case of tweaking the numbers to make sure it seamlessly moved to the correct position. The final step was to animate the swapped public colour being mixed with Alice and Bob's private colour. (see figure 14 screen grab 3) The same technique was applied by translating the private colours down the Y axis to the correct position then turning the private colour into the final colour, which was brown for both Alice and Bob. (see figure 14 screen grab 4)

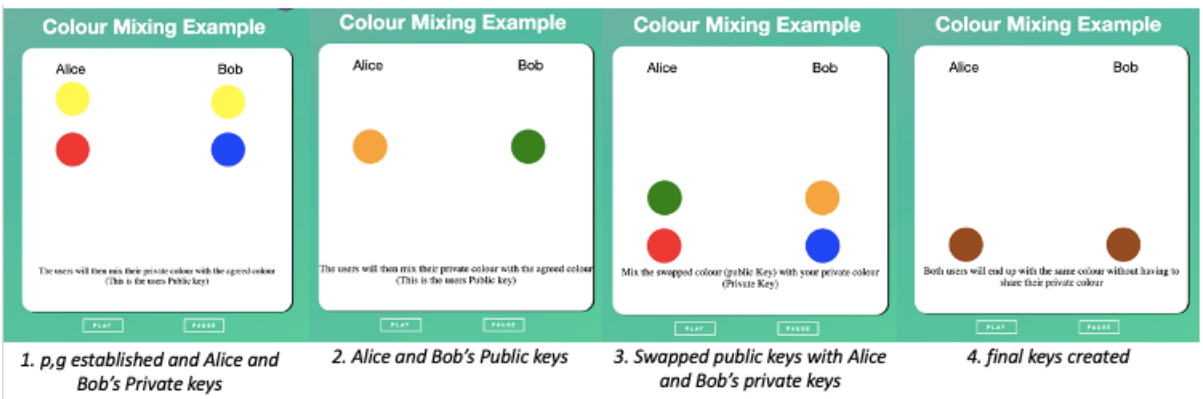


Figure 14-Animation process

4.2.2 Maths example implementation

The second timeline follows a very similar structure. This timeline is called MathsTimeline. However, in this animation the colour objects were replaced with the according equations that create the keys. Once viewing the animation, it was evident that it was quite hard to follow which equations were associate with each key. To solve this, it was decided to add dividing boxes around the equations. To make these boxes more dynamic SVG paths were used to create the outline of the box. SVG designs were very common when researching into animie.js and it was decided that the addition of these would be a nice addition to my animation, making the animation more complex and visually exciting. When researching open-source examples of DHKE a photo was identified as a clear and efficient way to explain the concept, therefore this as used as inspiration (see Appendix 5). A quality in this image which was attracting was how the design was split up the different mathematical calculations to make it clear which calculation equated to which key. This idea was mimicked in the implementation by creating SVG boxes with rounded corners encompassing the keys. When creating the SVG boxes no open-source solutions that fitted the design, therefore it was decided to implement it from scratch. This is an example of how the SVG boxes were implemented “<path class= "pathBob" d="M59,135 h100 a20,20 0 0 1 20,20 v20 a20,20 0 0 1 -20,20 h-100 a20,20 0 0 1 -20,-20 v-20 a20,20 0 0 1 20,-20 z" fill="none" stroke="orange" stroke-width="3" width="300" height="140"/>”. M59,135 let me control the location on the page that the box was positioned. The “h” values allowed me to alter the height of the box and the “v” values altered the width. Finally, to curve the edges of the box the “a” value was altered, and this defined the curve of the edge. (see figure 15) Once the box was created, the box was able to be manipulated easily to fit seamlessly into the design. Because the SVG are broken down into different coordinates it made animating this box very flexible. It was decided to animate the box, so it appears and snakes around the words as this looked visually dynamic. To animate this, the “strokeDashoffset” property was used. This determined where in the SVG the line snake would start and then the duration was set for how long the snake round would last. Finally, this was duplicated four times and placed the animation in the correct order within the timeline.

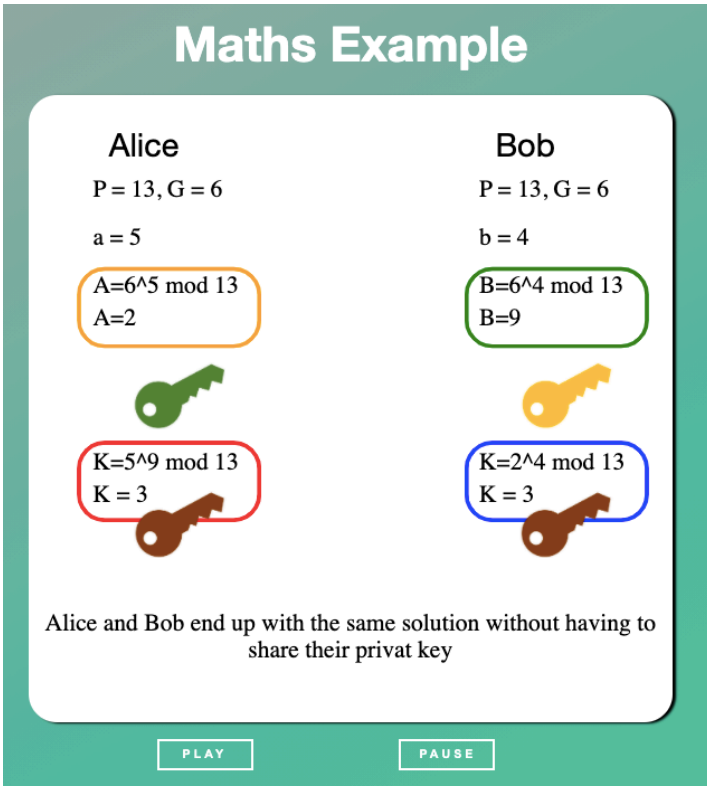


Figure 15-Fully ran animation of the maths example

The next issue to remedy was that the text moving across the screen looked messy and did not accurately reflect what was being sent. The text initially sent the whole calculation, when in reality only the solution would have been sent to the other user. Again, inspiration was drawn from the image found online. I liked how there was a key below the box which symbolised the 'key' that was going to be exchanged so it was decided to add this to the animation once the calculation was complete, to symbolise how the outcome was the key. To animate the keys clicking into place effect was added, this was achieved by rotating the key upward and back down again. Then the same process as the colour mixing example was followed and the keys moved diagonally across the screen to show the exchange of the keys. Together with the box it was believed that this successfully makes the maths calculations clearer and more effective. The rest of the animation followed the same structure of the colour mixing example, but instead of mixing the colours the calculations and resulting keys would appear.

The final timeline created was called introTimeline. This timeline was created to animate the 'prior play' objects in the GUI. This included objects such as the heading and the intro text. It was decided that it would be useful to have some text on the page before the user started the animation to help them decided what animation they wanted to view and understand a brief synopsis of the animation before watching it. To animate this synopsis the aim was to mimic old arcade games where 'press start' would flash up or hover on the screen. The hope was that this animation would be simple enough that it would not be too distracting, but still be entertaining enough to engage the user to use the website. The heading animation consists of two lines opening up to reveal the heading. The intention of this animation was to make the first thing the user sees have a professional impression and set the tone for the whole page.

There are three parts to this animation: the lines, the first half of the title, and then the second half of the title. (see figure 16) In the timeline the lines appear using the same opacity technique that was used with the objects above, however, to make the lines grow the line of code would be translated, this looked like: “translateY: (el, i) => (-0.625 + 0.625*2*i) + "em"”. Once the lines were in the fixed position, specific words appeared using a mix of the opacity technique and a translation left or right, depending on the alignment of the text. This Timeline is not triggered by a play or pause function from the user, instead it is in auto play once the page loads. The timeline is then on a loop three times as this was considered enough time for the user to make their decision on what animation they wanted.

Figure 16-animating the header

Once I was happy with all of these timelines and the flow of the animation, the next step was to merge the two examples in one page, with the maths example being to the left of the page and the colour mixing example aligned to the right. Once the two animations were merged, an issue appeared with the sizing. This was due to the CSS classes being set to the position ‘Fixed’. At the time of the development, when this issue was spotted the only thing that was done to fix it was to manually change the position of the classes. However, once realising this was a bigger issue than originally thought the class position were changed from fixed to absolute to make the page more responsive.

4.3 Deployment and Issues Faced

The animation was deployed on GitHub as this is a platform that all students will have experience using. Another added benefit of GitHub is the student account included free access to their ‘pages’ feature. This made the deployment of the website simple and meant that the website could be hosted on GitHub instead of another third party. The use of GitHub was also important as it additionally hosts the source code that the students could opt to download and run locally instead of online. To test out the deployment, the page was viewed the website on a screen that was not the screen that the animation was originally designed it on. The original screen size that the animation was created with was 13-inch while the secondary machines screen was only 11-inch. This posed a major issue at it cut off the bottom of the page where the play and pause buttons were positioned. This made the deployed website unusable as users were not able to control the animations (play or pause it) making the functionality of the animation inoperative. The animation must be accessible to all students and it cannot be assumed what size screen they own. Therefore, the code needed to be altered to make the webpage scalable and responsive.

Because most of the page is layout in different box formats, it was decided that a good solution to this problem was to put the whole page into a grid system. A grid system would provide the layout with an order for the elements on the page and can distribute them according on the priorities of the screen side. The grid layout also gave the animation more structure when the changes of position and sizing were made. This is due to the fact that the classes within the girds would not leave the maximum width of the assigned column and row. Different Div elements were used to divide up the different sections. Figure 17 displays the design that was created to visualise what areas will be in what grid format before it was implemented.

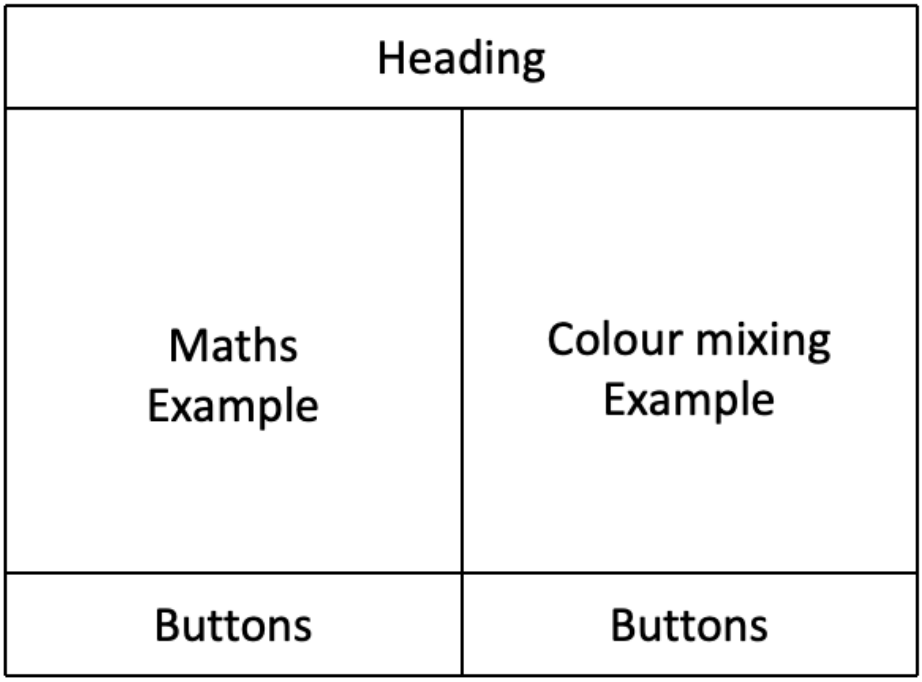


Figure 17-Gird layout design

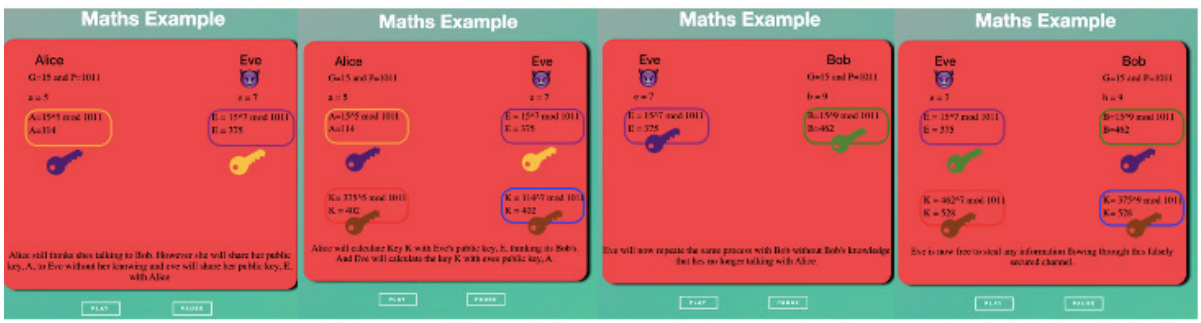
To make the page more scalable, the positions of each class were changed to absolute and the sizing of the units in each class were changed from px to vw. This represents the 'Viewport Minimum' and scales according to the height and width of the webpage. By changing the CSS and adding the gird layout the page became more scalable than the original.

4.4 Man in the middle attack implementation

The majority of the implementation was finished earlier than expected, resulting in having extra scheduled out time to work on the animations. To make the animations more informative and helpful for the students, it was decided to add in an additional animation page which explained how a man in the middle attack would occur for both examples. This addition is useful to students as this is another part of DHKE which is covered and examinable in the security module.

These animations were implemented on a separate page, which the user could navigate to via the devil emoji. This was decided due to the worry that four animations on one page would be too overwhelming and would result in the original animations to be smaller than intended. This could make it harder for the user to read the information in the animation. When making the man in the middle attack, inspiration was drawn from lessons in the security module and open-source information that gives more in detailed examples of a man in the middle attack. For continuity purposes, it was decided to keep the attackers name as Eve and also represented the attacker with a devil emoji, so it was very obvious that this person was malicious. The main build of the animation is a direct replica of the original DHKE examples, however in include Eve's presence and interception was included. In the maths and colour example once Alice and Bob are done creating their shared public key. In the man in the middle example Eve is introduced through text of her name appearing with the emoji. In addition to this the box which contains the animation turns into a deep red to again show the student watching the animation that an attack is taking place.

The first alteration that was made was in the maths example. Once Eve arrives on the screen, she intercepts Alice's key exchange. (see figure 18 screen grab 1) To visually represent this the key turns from orange to purple while it is travelling across the screen to Bob. The colour purple was chosen due to the fact that it mirrored the colour of the devil emoji. To show how the attack works two DHKE's occur; one with Eve pretending to be Bob and one where Eve is pretending to be Alice. To show this Eve takes over where Bob previously was, and the exchange carries on as normal without Eve suspecting a change. (see figure 18 screen grab 2) Once this exchange is completed the same occurs with Eve taking Alice's place. (see figure 18 screen grab 3) The rest of the animation runs as normal, but the calculations are all altered by Eve's interference. When the final keys are produced, Alice's and Eve have a brown key to symbolise the BHKE being complete, and Bob and Eve both have brown keys to show that the exchange between them was also successful. (see figure 18 screen grab 4) Eve ends up with two keys showing how she has successfully made two secure channels with both Alice and Bob. The same method was followed for colour mixing example. However, to make it obvious that two different DHKE occurred Alice and eve end up with brown final circles but Alice and Bob end with Black final circles. (see figure 19 screen grab 4)



1. Eve impersonating Bob

2. Eve successfully completing DHKE with Alice

3. Eve impersonating Alice

4. Eve successfully completing DHKE with Bob

Figure 18-maths man in the middle attack

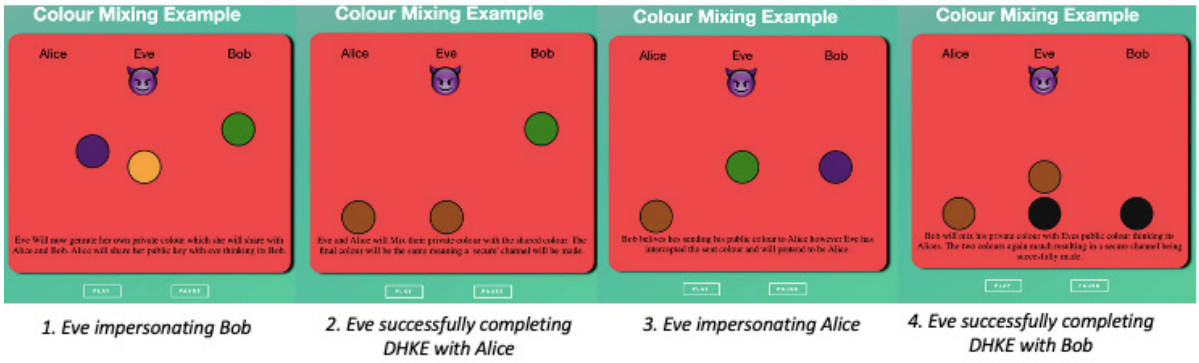


Figure 19-Colour mixing man in the middle attack

4.4.1 Issues faced during man in the middle attack implementation

An issue that was encountered while making the man in middle attack animation was, I initially interpreted the exchange differently to how it was taught in the security module. The initial animation showed Eve intercepting Alice's message and altering with her own key, which she then sends onwards to Bob, and vice versa with Bob to Alice. This would result in the final two equations to not equal together stopping the DHKE form working. However, this was not correct. I was basing my assumption off open source learning platforms and not getting the information directly from the security modules content. Doing that went against the aim of making a tailored animation for the students and gave me the wrong content to teach. After realising this mistake, in essence two DHKE's were happening: one between Alice and Eve pretending to be Bob, and the other with Eve and Bob with Eve pretending to be Alice. This meant that in this example Eve was making a secure channel with both Alice and Bob without their knowledge, and let Eve be free to steal any information flowing through this falsely secured channel. The change in the animation took a lot more time than originally anticipated as it meant having to re-visualise how the animation would flow and work. A hardship when designing the flow was how to reflect that Eve is pretending to be Alice and Bob at the same time, as in real time this would be simultaneous. In the end it was decided to show one exchange each with Eve and Alice with Eve taking the place of Bobs section on the page to represent her pretending to be Bob then doing the same thing with Eve. This constant movement was hard to animate as most of the objects were at different positions, so moving them all together would not work as it were not in line therefore, multiple duplicates of were created. Having duplicate objects made it easier to manipulate the objects to move as if an object was not originally inline, the duplicate could be placed so it was is the correct position. When changing the man in the middle attack it was made sure that the security module material was constantly being referred to. This made sure that the animation was accurate to the content being taught.

5. Results and Evaluation

5.1 Result of intended goals

To completely understand the full extent of how successful the project has been with achieving the goals, I will have to wait until the next year students start using the animation to help them learn about DHKE. This is due to the main goal and aims being that "that the retention rate of this material will increase and thus help students with their exam and application of this material.". However, I do believe that I have managed to meet a lot of the short-term goals that were set out to achieve with this project. The first and most important goal was to successfully "implement two animations that demonstrate Diffie Hellman, the first is a colour mixing example which is a common high-level way of explaining Diffie Hellman without going into detail about the underlying maths.". The final product involves 4 animations to demonstrate DHKE and the different security issues that could occur. During the user testing, 75% of participants found that the animations were clear and useful.

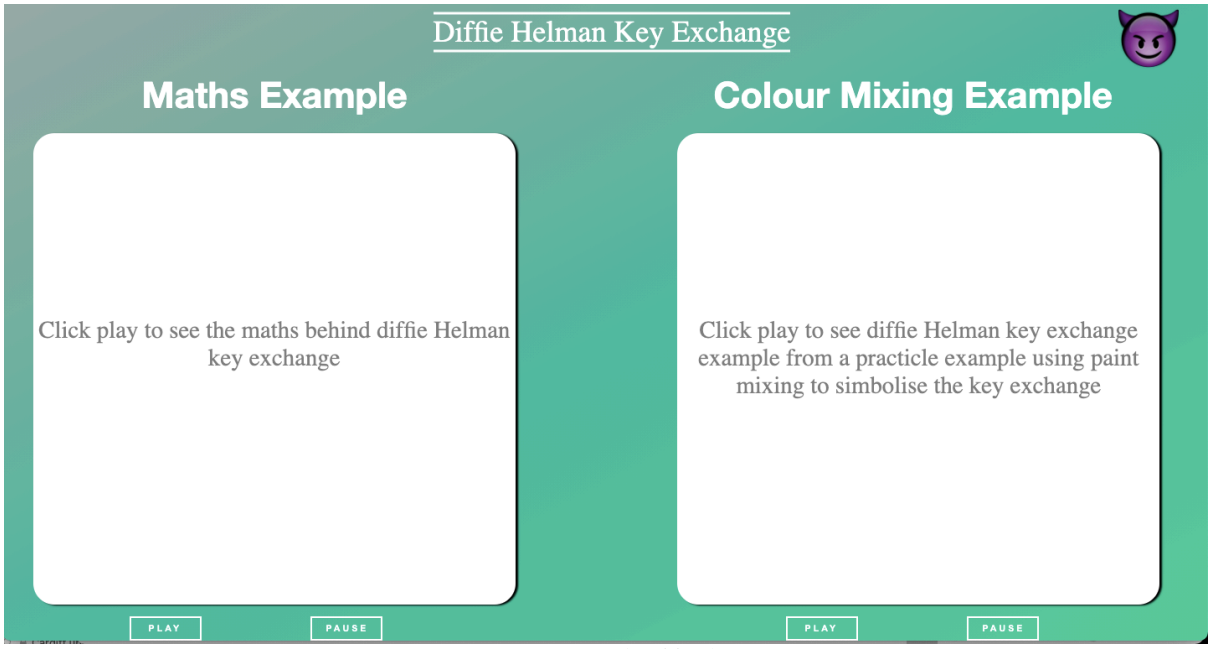


Figure 20-Example of final GUI

Another aim was to "create a user-friendly GUI to go along with the animations that will be deployed online to be accessible to all student studying the security module.". I incorporated techniques that were learnt form the second-year module HCI, my own experience with UI design, and background research from previous studies on animation tools for learning, which all helped me to produce a GUI that was user-friendly. Improvements can still be made on the GUI, highlighted by how some of the user feedback that was received expressed how they would prefer just one animation on each page instead of the dual animations that are currently implemented.

The final aim was “to create a study on retention rate of audible/visual learning and visual/ Kinaesthetic learning.”. This goal was not successfully fulfilled due to poor planning and not enough prior preparation. When initially making the Gantt chart, I was not aware of the time it would take to create the study and how important getting early ethical approval was. So, the task of getting ethical approval was put in the later stages of the project until the implementation was completed. This was due to the thought that the implementation took priority over the study. When the preparation for the study began there was 4 weeks left of the project which initially, I assumed would be enough time. However, to get ethical approval it could take up to two weeks for the request to be approved and I did not realise that the necessary documents needed to be prepared before you submitted for approval. This meant that when planning out the time management of the retention study, the documents were plans to be made while I was waiting for the approval to come back. This meant that materials such as the questionnaires, the consent forms, and the request email had to be made before the application for ethical approval could be submitted. This pushed but the request date for ethical approval to three weeks before the submission date meaning leaving only a a week to complete the study. The final week of my schedule was planned for writing the final report. I did not want to rush the study and I did not believe that in the time frame there would be enough time produced a study that was professional and accurate. Because this study did not occur as intended, it has been added into my future work. This is due to the fact that the study is important to understand whether the current teaching techniques are fulfilling the needs of the students, or if new methods should be implemented.

5.2 Testing

To test the final product, a range of techniques were used to understand any unforeseen issues or changes that should be applied. The three main tests that were administered were ‘Functionality Testing’, ‘User Testing’ and Security Testing.

5.2.1 Functionality Testing

The first type of testing what was performed on the implementation was functionality testing. The aim of this testing is to “test each function of the software application, by providing appropriate input, verifying the output against the Functional requirements.”[14] To test the functionality, a table was created which defined the specifications, Steps to execute, expected outcome and then the status (see table below). The different Test case status definitions are defined below.

Test Case status definitions are:

Passed (P): Test matches the expected result.

Failed (F): The test did not match the expected result. In some cases it did run but another issue arose from the test.

Not Run (NR): Test has not yet occurred.

Unsure (U): Test has been run its unsure if it passed or failed test. This will be investigated

Test No.	Specification	Steps to Execute	Expected Outcome	Status
1.	The user will be directed to the home page when the specific URL is clicked, and it will load the HTML page with the animations.	1.click the link 2.user should be redirected to the page	The animation of the Title and Info summary will start and both boxes will be present	P
2.	User can use the Play Button on the Maths example to starts the animation.	1. Hovering over the start button displays the Play icon. 2. Button is pressed 3. The maths animation Begins	The animation begins once the button is pressed.	P
3.	User can use the Pause Button on the Maths example to pauses the animation.	1. Hovering over the Pause button displays the Pause icon. 2. Button is pressed 3. The maths animation Stops at current placement.	The animation pauses once the button is pressed.	P
4.	User can use the Play Button on the Colour Mixing example which will start the animation.	1. Hovering over the start button displays the Play icon. 2. Button is pressed 3. The colour mixing animation Begins	The animation begins once the button is pressed.	P
5.	User can use the Pause Button on colour mixing example to pauses the animation.	1. Hovering over the Pause button displays the Pause icon. 2. Button is pressed 3. The colour mixing animation stops at current placement.	The animation pauses once the button is pressed.	P
6.	User can redirect to the man in the middle attack page.	1. User clicks on the devil emoji 2. The user is redirected to the man in the middle attack page 3. The page is present, and the header and info text animations start.	The page gets redirected to the man in the middle page. (middle.html)	P
7.	User can use the Play Button on the Man in the middle maths example which will start the animation.	1. Hovering over the start button displays the Play icon. 2. Button is pressed 3. The man in the middle maths animation Begins	The animation begins once the button is pressed.	P
8.	User can use the Pause Button on man in the middle maths example to pauses the animation.	1. Hovering over the Pause button displays the Pause icon. 2. Button is pressed	The animation pauses once the button is pressed.	P

		3. The man in the middle maths animation stops at current placement.		
9.	User can use the Play Button on the Man in the middle colour mixing example which will start the animation.	1. Hovering over the start button displays the Play icon. 2. Button is pressed 3. The man in the middle colour mixing animation Begins	The animation begins once the button is pressed.	P
10.	User can use the Pause Button on the man in the middle colour mixing example to pauses the animation.	1. Hovering over the Pause button displays the Pause icon. 2. Button is pressed 3. The man in the middle colour mixing animation stops at current placement.	The animation pauses once the button is pressed.	P
11.	User can redirect to the Home page via the home button.	1. User clicks on the home icon 2. The user is redirected to the home page. 3. The page is present, and the header and info text animations start.	The page gets redirected to the home page. (current.html)	P

5.2.2 User Testing

The second testing that was performed on the website was the user testing. Participants that volunteered to be a part of the testing were sent a google form's questionnaire containing questions about the animations. This questionnaire was anonymous, so the users would be as honest as possible. Google forms was used as it was the most accessible way of distributing these questionnaires (see Appendix 6). The first question in the questionnaire asks: 'Have you learnt about Diffie Hellman Before?'. This was important to distinguish because the background knowledge of DHKE may make it easier to understand the animations, and as my animations are targeted to students that are learning about DHKE it is important for me to see that the people who have not studied DHKE before still understand and enjoy the animations. From the 4 participants, 75% of them had previous knowledge of Diffie Hellman and 25% had not studied it before.

The next question was 'did you think the animations were clear?'. This is an essential question as the main purpose of the animations was to aid learning and retention rate of DHKE. If these animations are not clear, then the student's ability to learn the information may be negatively impacted. For this question there were three response options: Yes, No, and sort of. 75% percent of participants said yes and 25% said 'sort of'. It was interesting to me to see that the person who said that they have not learnt DHKE before was the person who responses to the second question with sort of. This means that 100% of the people who had previously learnt DHKE found the animations clear, but for someone with no background knowledge found it more difficult to fully understand the concept. The target audience for

this animation will be students who are currently learning about DHKE, so while making the animations the assumption was present that the student would have some knowledge of the basic concepts of DHKE. Nevertheless, it is important that this is more accessible to everyone. To understand how the animations could be clearer, the question 'What could be added to make the animation clearer?' was asked to the participants. The user who had not previously answered 'sort of' responded to this question with 'Maybe additional info on the circles to show if they're private or public.'. This made me believe that maybe the colour mixing example was where they struggled to understand the concept. Therefore, in my future work there will be an emphasis put on make the colour mixing example clearer by identifying what each colour represents. Other responses to 'What could be added to make the animation clearer?' were 'various in text colours, fonts or bold' and 'Unsure of the scope of the animation but adding an overview of DHKE and the point of it would make it clearer in my opinion for those who are new to it.' I agree with the latter comment that maybe some content before the animations may be helpful to give the students more theory behind why DHKE is useful/ needed. This was not initially displayed this on the website as there was the concert that this type of background information is covered in the security module and the animations is more for examples than theory. This is something may be considered adding in the future work if students voice that they will benefit form more background.

Next, 'Do you think the animation is a good speed' was asked to the participants. This was a question that was necessary to ask to make sure the users found they have enough time to read the narration while also watching the animation take place. 100% of the participants said yes, they thought the animations went at a good speed. The next question asked, 'do you like the layout of the animation?'. This was asked to see if the requirement to have a 'user-friendly GUI' was successfully met. The response options for this question were: Yes, no, and could be improved. In response to this, 50% said that they did like the layout and the other 50% said it could be improved. When the users were prompted to say, 'How would you change the layout to make it easier to use (if any changes)' a lot of the responses referred to how they did not like how the design of the webpage had two animations on one page and that it would be better to have them on separate pages. One user said, 'I like that you can compare the animations at the same time, but I would like an option to see one animation per screen' and another said, 'I didn't like the dual animations.' The first comment highlighted a solution to this problem which could implement in the future. To combat this layout, issue the implementation of an option function on the home page should be included. This would result users being able to choose how they want to view the animations. These options could include single view or dual view.

To fulfil the same requirement of having a 'user-friendly' GUI it was important to make sure that the navigation of the GUI was intuitive and clear. To find out if this requirement was met the question 'Did you find it easy to navigate to the man in the middle attack page' was asked to the participants. 100% of participants said they found it easy to navigate to the man in the middle page reassuring me that the navigation of the website was clear.

The participants were asked 'Which animation did you find most useful'. The response options for this question were: Maths Example, Colour mixing example, Maths's example (man in the

middle attack), Colour mixing example (man in the middle attack) and all of the above. 50% of the participants responded with 'Maths's example (Man in the middle attack)' and the other 50% responded with 'all of the above'. This confirmed the assumption that the users found the maths examples clearer than the colour mixing example, and that extra narration or representation like assigning the circles clearer names will be needed in future implementations to make this animation more useful. In addition, a follow up question was asked: 'is there any other functionality you would like to see?'. This was to make sure that the users got everything possible out of the animation and if they felt like something was missing this could be recorded and added into the next implementation. All the responses to this question were that 'no additional functionality needs to be added'. This indicates that the solution has successfully met my requirement of making a security animation that represents DHKE.

5.2.3 Future Tests

Additional testing which would be useful to stop any flaws or issues in the system that would be useful to perform but were outside of the project scope due to a lack of time and resources include testing such as Load Testing and Compatibility Testing. Load testing is an important test to see how the system hold up with multiple people using the system at the same time. As the system will be accessible to a whole module class, there is a high change that multiple students will be on the system at the same time, therefore it is important to make sure that issues will not occur while this is happening. Another helpful test would have been compatibility Testing. During the implementation there were serval issues with the capability as the GUI was not responsive enough to work on different size screens. Even though most of the issues with scaling were combatted during the implementation, this testing would still have been useful to identify and missed issues. This testing was not possible within the scope of my project as it would require me having access to multiple devices of different sizes, and different search engines were not available to me. Due to Covid-19 computer science labs and equipment were not accessible to me as I have stayed at home to complete the project. This testing is important to complete in the future as all students have their own preference on devices to use while studying and the web browser they use, thus it is important that the application is available and compatible with all different platforms and if they are not compatible, it should at least be clear to students' which platforms the project is not available. Currently the website has only been tested on Safari, Chrome, a 13-inch screen and an 11-inch screen.

5.2.4 Reflection after Testing

Through the testing process I have been able to identify the strengths and weaknesses of my solution. The strength of the system includes that the flow of the animation seems to be appealing and functional to all users, the speed of the animation is paced well, and the narration and visuals were well received. Another strength is that all the basic functionality works and is intuitive to the users. All the participants of the testing found it easy to navigate through the page and run each of the animations. The system also passed all of the basic functionality testing that were performed. Some of the weaknesses that were identified included cosmetic issues, such as the layout of the system was not pleasing to all participants. This could be solved

by implementing an option feature where the user can choose how to view the animations before they play them. This means that the layout can be tailored to the user and their preferences. It was also identified that most participants preferred the maths examples to the colour mixing examples, so in the future the addition of headings in the animation would help the users understand what colour is associated to what key.

6. Future Work

There are lots of cosmetic and functionality changes that be beneficial to add to the system if more time was allocated to the project. Due to Hofstadter's Law: 'Everything takes longer than you think, even when you take into account Hofstadter's Law.' Many of the intended ideas were not made into fruition due to a lack of time or realising these concepts and ideas too late in the process to implement. A requirement that was not achieved was the retention study which compared how well students retained DFKE from text in comparison to my animation. The inability to complete this requirement was due to a range of issues but was mainly due to poor preparation leading to a lack of time. As mentioned in the results and evaluation section, when I started preparing for the study there were 4 weeks left of my project which I assumed would be enough time, however the necessary ethical approval taking longer than expected resulted in not enough time to complete the study. In the process of preparing for the study I produced both questionnaires and all the necessary documentation, so this study will be achievable to do in the future. The end goal of this study was to gather the data from both questionnaires and compare the success rates to the questions to see which group did better, the text only group or the animation group. Hopefully this could help prove if my project successfully improved the retention rates for students as this was my main aim for the project.

In the future, a priority will be to add extra functionality into the animation. Most notably, I would want to add more features that would allow the user to interact more with the animation. This would involve implementing user input boxes where they could input their own numbers for P, G and/or a,b, resulting in the students have a better understanding of how different numbers will affect the outcome, and how the numbers are chosen. This was not initially put this into the implementation due to it being outside of the project scope and there were concerns that it would turn a learning tool into a way for students to cheat and just input the desired numbers without actually understanding the theory behind it. On reflection, I think that this would be a helpful feature alongside the theory and passive learning is not always very effecting so getting the users to interact with the animation might increase their understanding of the theory.

The user testing highlighted further design and layout changes that could be implement into my animation. The user testing was conducted towards the end of the project, resulting in not enough time to implement the suggested solutions, but If I had more time, this would be a priority. From the user feedback, some participants did not like the layout of the animations and found that having one animation per page would be better. To solve this issue, an additional feature could be added that gave the user the options to choose the layout of the animation. The user would have the ability to choose between a single animation or the dual animation. This gives the user more control of the tool and will hopefully improve their experience as it will be more tailored towards their preferences while learning. It was also evident from the user feedback that the maths examples were better received then the colour mixing example. To improve the legibility of the colour mixing example it was suggested that labels were added to the colours to show what key they each represent.

7. The Conclusion

To solve a problem that students do not having enough tailored revision and e-learning material during the covid-19 period, it was anticipated to create a security animation aimed at final year students who are taking the module security. The security module would display how the cryptography technique DHKE works through a maths example and a colour mixing example. The first aim was to gain a better understanding of the psychology behind learning and apply this research to the animation. This was successfully achieved through looking into different literary papers that performed studies on how animation effected retention rate and learning. From my research, this learnt knowledge was added to the design to create a minimal design for the animation so users would not be overwhelmed. From the background research I successfully added narration to my animation with the aim that it would 'encourage learners to make a connection between corresponding elements in the two representation' (Björn B. de Koning*, Huib K. Tabbers, Remy M.J.P. Rikers, Fred Paas). This background research drove the techniques and practices to put into place to make the animation as effective and pedagogical.

Another aim that was successfully achieved was to create a user-friendly GUI. This was accomplished by implementing HCI techniques to make the design as visually appealing and intuitive as possible. Feedback from the participants was overwhelmingly positive and proved this goal was successful. Additional features and improvements were highlighted in the feedback which will be applied in future work. The animation was successfully implemented. All the necessary features were present including the addition of two extra animations. In the implementation I was able to achieve more then was set out in the initial plan.

The aim of performing a retention study of students who learnt DHKE thought a textbook Vs the current animation was not successful. With more time this would be the main task to carryout.

Most aims that were set out in the initial plan were fully realised and created with the exception of the retention study. Overall, this project is viewed as successful and will be able to be implemented in the available e-learning tool set come next year. This will give students greater options of how they learn the content taught to them and provide them with more tailored revision material.

8. Reflection

Through this project I have managed to learn and developed new skills and practices. A key skill that I learn was the language of animie.js. I researched this on my own and the language was self-taught throughout the process. The use of documentation and online examples helped my understanding and development with this skill. In addition to the simple skills that I have learnt, I have additionally identified transferable learning, which can be carried over into future learning. An example of this is how to deal with third party stockholders while creating a project. The stakeholder in this case was the ethics committee. I needed to get ethical approval for my user testing, however this was only filed for towards the end of my process, assuming it would not take long for a response and approval. However, the process turned out to be a slow and complex one requiring multiple emails to confirm the correct documentations were made and the need for them to go to a fortnightly meeting to accept these documents. This resulted in my timings for my retention study to be pushed back to a point where creating the study would have been to rushed and non-beneficial. In the future it is important that when working with third parties that these kinds of requests and contacts are established from the beginning of the process to make requests more seamless.

When it comes to user feedback, I learnt that I should look more deeply into what the root causes are, and not just make surface level cosmetic changings thinking this will solve my issue. Regarding the colour mixing example, I should have started from scratch and asked the users more what they did not understand with the colour mixing to make sure that that example is just as useful as the maths example. Instead, all I changed was the layout of the page thinking that if the users watched the maths example first then the colour mixing example would be easier to understand. On reflection, this change was not dramatic enough to actually make the colour animation any more comprehensive. I should have made a bigger change of how I represented the colour mixing example rather than just a simple layout change. The issue ran deeper than a cosmetic issue and this was reflected in my user testing at the end, that even with the layout change the uses still found the colour mixing example hard to follow. This also highlights to me that the agile methodology that I adopted was not used to its full capacity. User testing twice was only produced throughout the process and on reflection if I got user feedback more regularly then some problems that I encountered much could have been solved much faster.

I learnt that the use of a variety of testing techniques would have enhanced my application and reduced the chance of unexpected issues appearing at the end. An example of a testing technique that I did not use, but should have, was compatibility testing. Performing these tests throughout my project would have identified the scaling issue much early on, and this would have allowed me to not waste as much time fixing all of the existing fixed position code I had in place.

In the early stages when designing the application, it was decided to not make the animation interactive and more of a static video. If this could be done again, I would make sure the user had more freedom and flexibility within the system as this would encourage the user to put what they learnt into practice and use the tool multiple times. When predicting the users return rate, I believe this will be quite low due to the animation being unchanging and that by viewing it again they will not gain any extra information that differs from their first experience. On reflection, with a learning tool such as this it would be more appropriate to have a more interactive and diverse range of options for the user to choose from. However, I do believe that the website I have produce successfully meets all my requirements and is a good starting point ready for more features if I had the time and the resources. The lessons and experiences I have encountered during this project will be carried thought into my later life and will I endeavour to apply these to the projects I work on in the future.

Table of Abbreviations

Abbreviation	Explanation
DHKE	Diffie-Hellman Key Exchange
GUI	Graphical User Interface
HTML	Hypertext Markup Language
CSS	Cascading Style Sheets
NSS	National Student Survey
MVP	Minimal Viable Product

References

[1] Lunden, I., 2020. *TechCrunch is now a part of Verizon Media*. [online] Techcrunch.com. Available at: <https://techcrunch.com/2020/02/19/online-learning-marketplace-udemy-raises-50m-at-a-2b-valuation-from-japanese-publisher-benesse/?guccounter=1>

[2] St. Louis, M., 2017. *How to Spot Visual, Auditory, and Kinesthetic-Learning Executives*. [online] Inc.com. Available at: <https://www.inc.com/molly-reynolds/how-to-spot-visual-auditory-and-kinesthetic-learni.html>

[3] Dr. George Theodorakopoulos. Security Module description. Available at: https://data.cardiff.ac.uk/legacy/grails/module/CM3110/20A.html

[4] Daniels, D., 2019. *Why is Visual Learning So Important?*. [online] Insight Resources. Available at: https://www.insightresources.org/2019/04/26/why-visual-learning-and-teaching/

[5] TavakoLi, M. and Gerami, E., 2013. *The Effect of Keyword and Pictorial Methods on EFL Learners' Vocabulary Learning and Retention*. [online] ResearchGate. Available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjWvbaCk7fvAhWAQkEAHXLoA4UQFjAAegQIAxAD&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4594874.pdf&usg=AOvVaw2ocaV4D4b9X6KydnHV7qR6> [Accessed 10 May 2021].

[6] En.wikipedia.org. n.d. *Diffie–Hellman key exchange - Wikipedia*. [online] Available at: <https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange>

[7] Boucheix, J. and Richard, L., 2010. *An eye tracking comparison of external pointing cues and internal continuous cues in learning with complex animations. Learning and Instruction*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/222567777_An_eye_tracking_comparison_of_external_pointing_cues_and_internal_continuous_cues_in_learning_with_complex_animations/link/5daff12c92851c577eb9befd/download

[8] de Koning, B., Tabbers, H., Rikers, R. and Paas, F., 2010. *Learning by generating vs. receiving instructional explanations: Two approaches to enhance attention cueing in animations*. [ebook] Elsevier. Available at: <https://www.sciencedirect.com/science/article/pii/S0360131510000710>

[9] Cooke, G., 2020. *Online learning vs face to face learning*. [online] Elucidat. Available at: <https://www.elucidat.com/blog/online-learning-vs-face-to-face-learning/>

[10] Paul, J. and Jefferson, F., 2019. *A Comparative Analysis of Student Performance in an Online vs. Face-to-Face Environmental Science Course From 2009 to 2016*. [online] Frontiers. Available at: <https://www.frontiersin.org/articles/10.3389/fcomp.2019.00007/full>

[11] Dr. George Theodorakopoulos. Security Module description. Available at: https://data.cardiff.ac.uk/legacy/grails/module/CM3110/20A.html

[12] tylerl, (username)., 2013. *"Diffie-Hellman Key Exchange" in plain English*. [online] Information Security Stack Exchange. Available at: https://security.stackexchange.com/questions/45963/diffie-hellman-key-exchange-in-plain-english

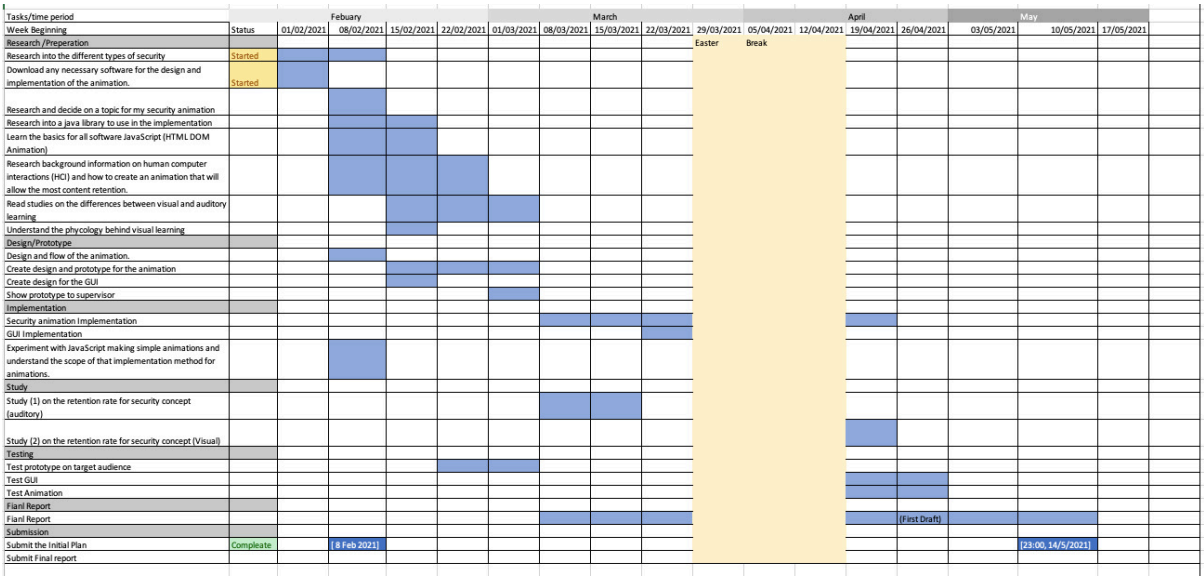
[13] Buchanan, W., 2021. *diffie*. [online] Asecuritysite.com. Available at: <https://asecuritysite.com/encryption/diffie>

[14] Guru99.com. 2021. *What is Functional Testing? Types & Examples (Complete Tutorial)*. [online] Available at: <https://www.guru99.com/functional-testing.html>

To view the working animation which is hosted on GitHub:
https://c1705987.github.io/DHKEanimation/current.html

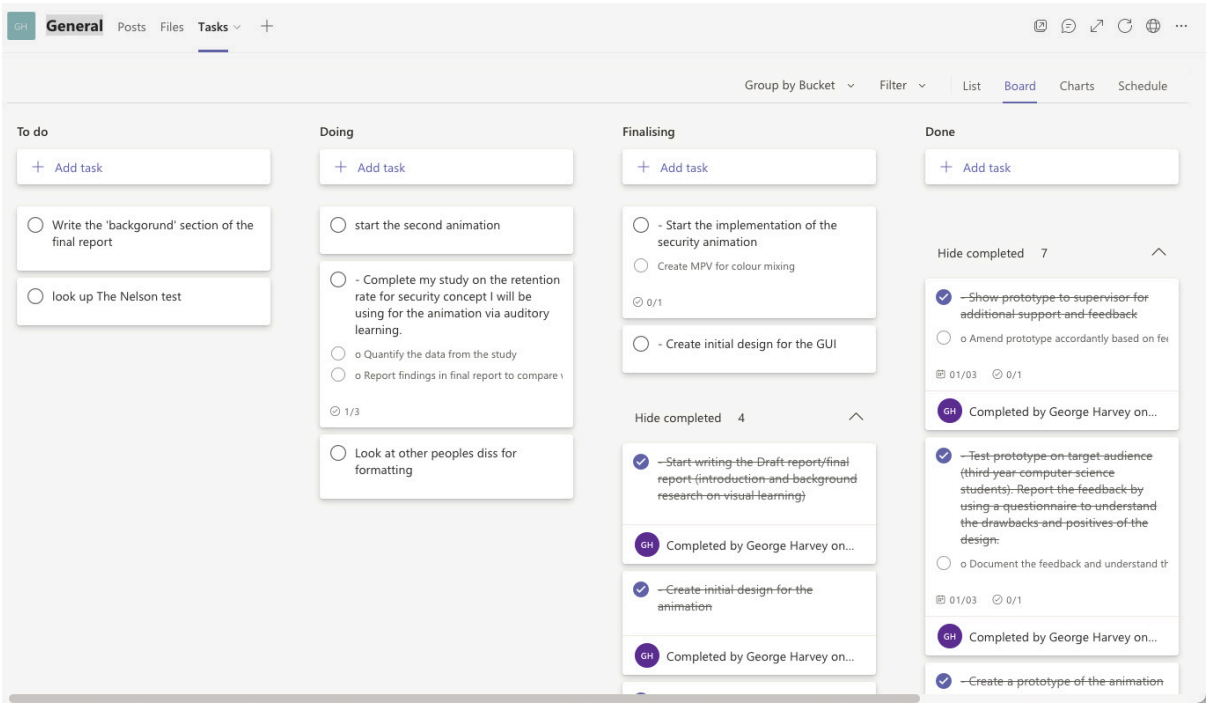
Appendix

Appendix 1

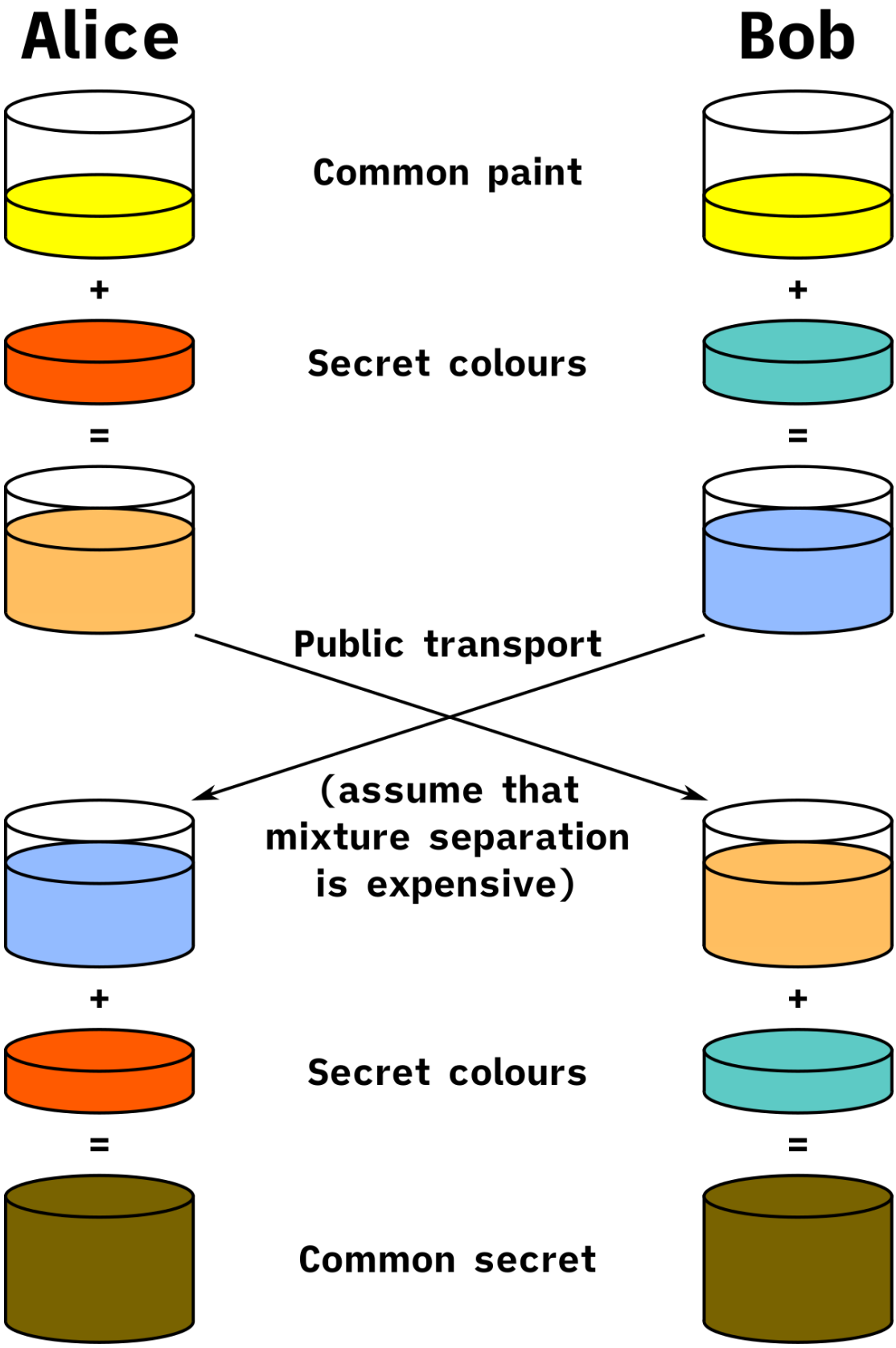


Tasks/time period		Febuary				March					April			May		
Week Beginning	Status	01/02/2021	08/02/2021	15/02/2021	22/02/2021	01/03/2021	08/03/2021	15/03/2021	22/03/2021	29/03/2021	05/04/2021	12/04/2021	19/04/2021	26/04/2021	03/05/2021	10/05/2021	17/05/2021
Research /Preperation										Easter	Break						
Research into the different types of security	Started																
Download any necessary software for the design and implementation of the animation.	Started																
Research and decide on a topic for my security animation																	
Research into a java library to use in the implementation																	
Learn the basics for all software JavaScript (HTML DOM Animation)																	
Research background information on human computer interactions (HCI) and how to create an animation that will allow the most content retention.																	
Read studies on the differences between visual and auditory learning																	
Understand the phycology behind visual learning																	
Design/Prototype																	
Design and flow of the animation.																	
Create design and prototype for the animation																	
Create design for the GUI																	
Show prototype to supervisor																	
Implementation																	
Security animation Implementation																	
GUI Implementation																	
Experiment with JavaScript making simple animations and understand the scope of that implementation method for animations.																	
Study																	
Study (1) on the retention rate for security concept (auditory)																	
Study (2) on the retention rate for security concept (Visual)																	
Testing																	
Test prototype on target audience																	
Test GUI																	
Test Animation																	
Fianl Report																	
Fianl Report														(First Draft)			
Submission																	
Submit the Initial Plan	Compleate		[8 Feb 2021]													[23:00, 14/5/2021]	
Submit Final report																	

Appendix 2



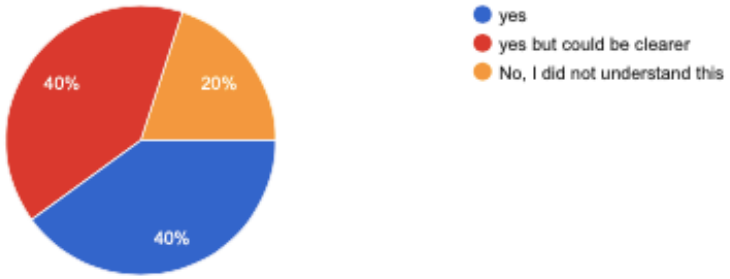
Appendix 3


Alice
Bob
Common paint
+
+
Secret colours
=
=
Public transport
(assume that
mixture separation
is expensive)
+
+
Secret colours
=
=
Common secret

Appendix 4

Do you think the animation of the colour mixing is clear

5 responses



If you answered anything other than yes please expand on your answer

3 responses

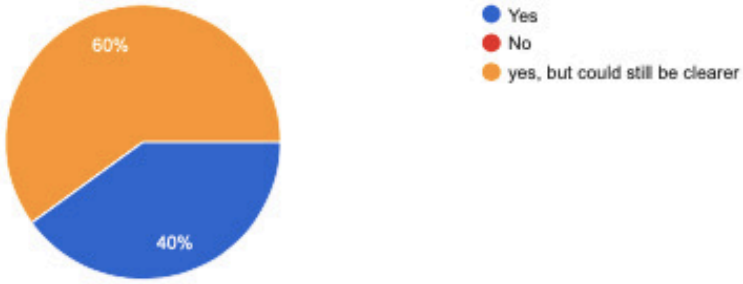
Add some writing on screen like the numerical one :)

Using my non compsci brain this isn't really explaining much. I do however love the concept of mixing the two different colours to make the same colour. With an addition of some extra explanation this could be an ace way of animating the exchange.

Its not super clear when the colours reappear from the bottom where they have been

Do you think the animation of the mathematical key exchange is clear

5 responses



If you answered anything other than yes please expand on your answer

3 responses

When the animation changes in the numerical key exchange (K=Abmodp to K=2Amod13) it may need some explanation or indication as to where the substitute numbers are coming from. same for other parts. Perhaps add in a few lines or arrows that appear that indicate where the number is coming from.

When numbers are substituted into equations, it should still be possible to see what the equation was before numbers were substituted. This could simply be done by placing the substituted version of the equation below the already existing equation.

I think it could be useful to show the colours merging together, it would be a nice touch in my opinion. It is difficult to fully grasp the clarity of the animation without understanding the assumptions of what your target audience knows. For a student like myself I understand it, but for someone who doesn't know basic concepts it would be trickier. More specifically the mod sections (why mod?) but I am sure you have that sorted elsewhere.

what's your thoughts on the design of the animation and is there anything else you would add

5 responses

Again, just add in some lines or arrows to indicate where numbers fit in the place of letters (if that makes sense). Also i would put the writing in boxes and list them as steps like: 1) agree on 2 numbers.. and so on. I would also make each part a bit more separated step wise so that its spaced out a bit clearer. I.e. Two columns differentiated by column boxes for Bob and Alice so we can see them as two different people. Then when various areas merge or switch over between the two, they can travel in the empty space areas.

Seems clear enough, maybe use something different than the falling letters.

Basic looking, as you are aware. But it is effective. As mentioned above the colour aspects I think are really nice touch and I definitely would stick with that. But maybe you could explore more 3D looking apporaches to make this stand out from the crows.

I liked it, I've never seen it explained with colour. Good for visual learners.

The paint splatters don't seem particularly relevant to the topic?

Is there any other functionality or animations that would help you better understand Diffie Helman key exchange

5 responses

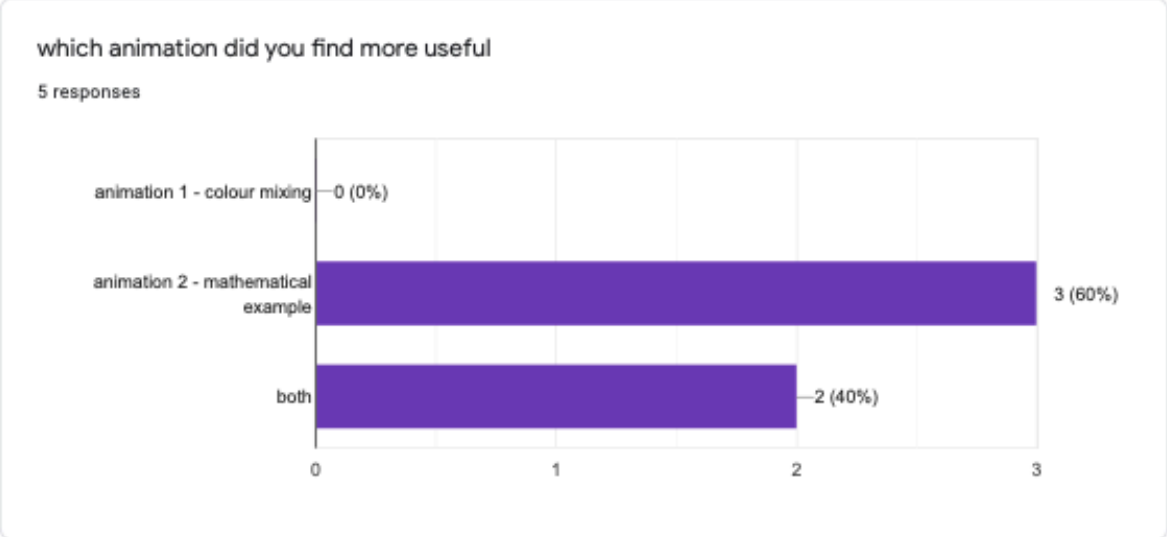
Add writing and steps like the numerical one on screen so its clear what is happening and why it is happening. Perhaps do the same as suggested above with making both Alice and Bob super separate through coloured columns or maybe an icon for each of the people. The icon can stay static on screen but it might help. By icon i mean like an outline of a person or something.

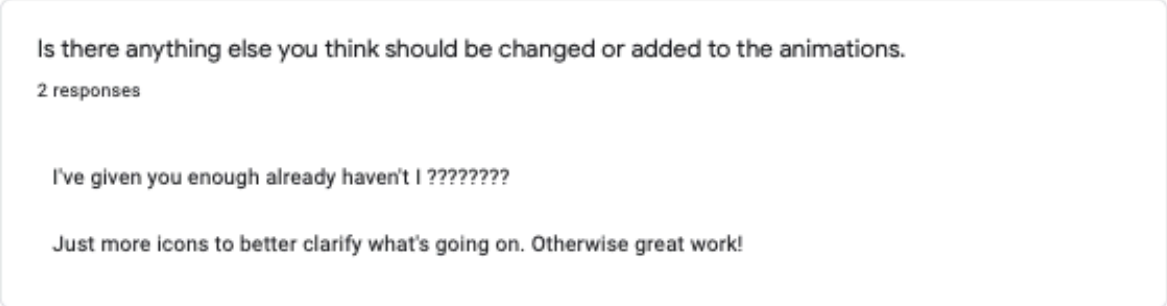
No, this example is clear enough.

A cool idea I thought of is showing a 'real life' version of the exchange to make visualising easier. Prehaps have two people throwing a key over a lake and in the lake. The lake could then have an interceptor, if you are exploring that avenue. Personally, that route would excite me more and for a younger audience could keep them engaged and help their learning.

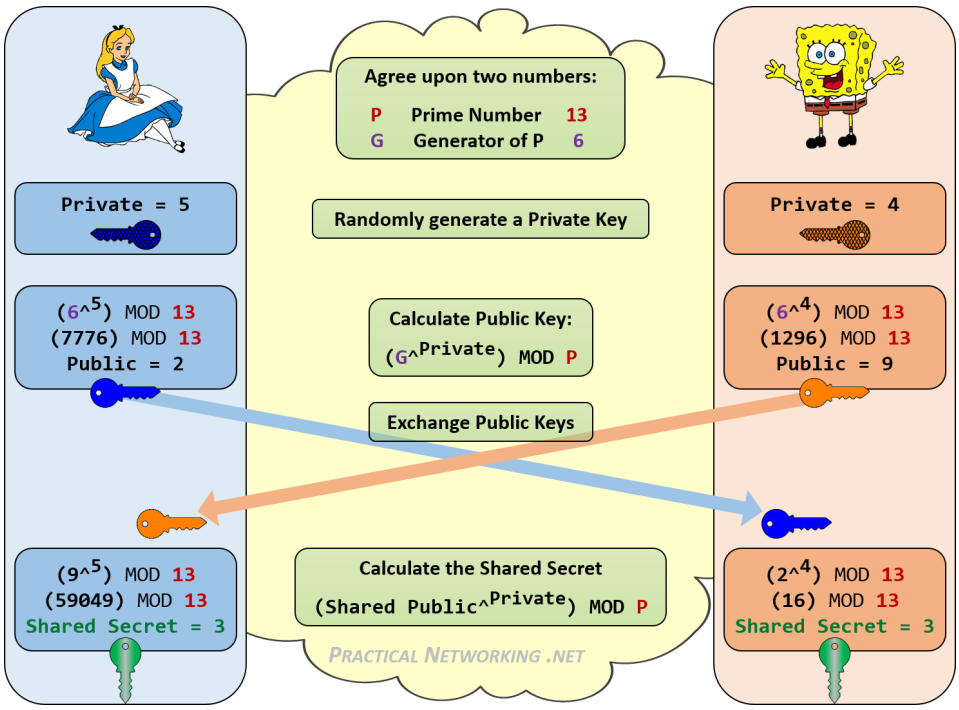
N/A

Maybe more icons showing like sending from one pc to another rather than just lines with no context


which animation did you find more useful
5 responses
animation 1 - colour mixing
0 (0%)
animation 2 - mathematical example
3 (60%)
both
2 (40%)
0
1
2
3


Is there anything else you think should be changed or added to the animations.
2 responses
I've given you enough already haven't I ????????
Just more icons to better clarify what's going on. Otherwise great work!

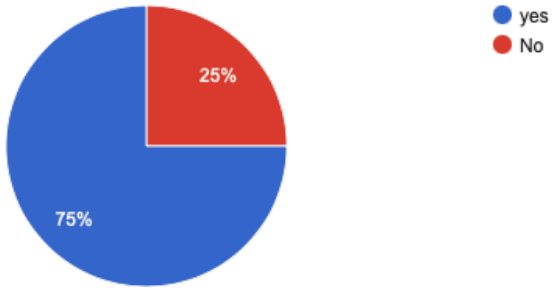
Appendix 5


Agree upon two numbers:
P Prime Number 13
G Generator of P 6
Private = 5
Randomly generate a Private Key
Private = 4
(6^5) MOD 13
(7776) MOD 13
Public = 2
Calculate Public Key:
(G^Private) MOD P
(6^4) MOD 13
(1296) MOD 13
Public = 9
Exchange Public Keys
(9^5) MOD 13
(59049) MOD 13
Shared Secret = 3
Calculate the Shared Secret
(Shared Public^Private) MOD P
(2^4) MOD 13
(16) MOD 13
Shared Secret = 3
PRACTICAL NETWORKING .NET

Appendix 6

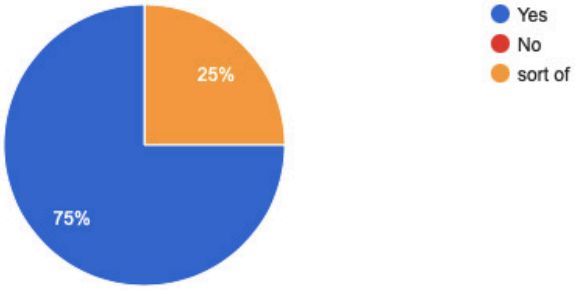
Have you learnt about Diffie Helman Before?

4 responses



did you think the animations were clear?

4 responses



What could be added to make the animation clearer

3 responses

Unsure of the scope of the animation but adding an overview of Diffie Helman and the point of it would make it clearer in my opinion for those who are new to it.

various in text colours, fonts or bold

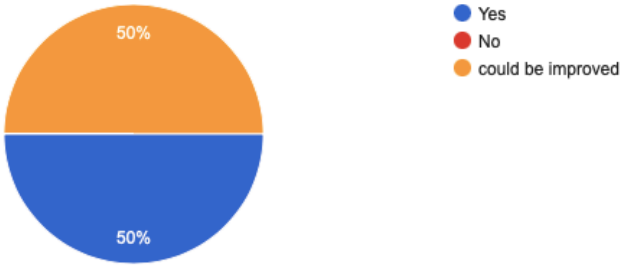
Maybe additional info on the circles to show if they're private or public.

Do you think the animation is a good speed

4 responses

do you like the layout of the animation

4 responses



How would you change the layout to make it easier to use (if any changes)

3 responses

I like that you can compare the animations at the same time but I would like an option to see one animation per screen.

An introduction about the basic concept and which to run first

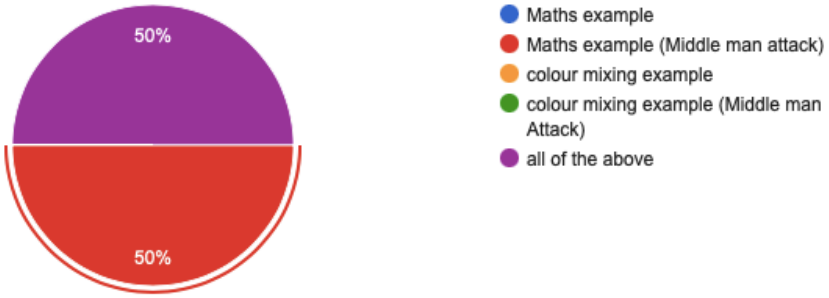
I didn't like the duel animations

Did you find it easy to navigate to the middle man page

4 responses

Which animation did you find most useful

4 responses



is there any other functionality you would like to see?

2 responses

I don'y see the need for any additional functionality

no

And extra feedback

4 responses

It was very helpful to have both a mathematical example and more visual example. Although I did find the middle man page it wasn't immediately obvious that the emoji was a link

N/A

it was a good animation

I found the maths example easer to follow as it used coloured key icons. I found this a better symbol to refer to a key rather than a coloured circle. A coloured key icon is better than a coloured circle in my opinion

Appendix 7

Q7. Alice wants to execute Diffie-Hellman Key Exchange with Bob. Given a prime modulus p, a primitive root g of p, and Alice's and Bob's secrets (A and B, respectively), show the steps of DHKE. [8]