UNIVERSITY OF WOLLONGONG

Bachelor of Computer Science - Digital Systems Security

CryptBase

Trapdoor Knapsack Simulator

Project Report

Presented by CSCI321-SSP19_2C

WU CHUJUN (5988329)

CHONG JIAHAO (4799276)

MARCUS TAN YONGHUA (6212621)

KYAW MYO AUNG (6097868)

<Project website: *https://cryptbase321.wixsite.com/home/blog/>*

Document version control

Date	Version number	Description
19/08/2019	1.0	Document creation
20/08/2019	2.0	Content updated
21/08/2019	3.0	Content updated
22/08/2019	3.1	Content Formatting
23/08/2019	4.0	Content updated

Table of Contents

1. Vision

1.1. Project overview

To create a simulator that run trapdoor knapsack algorithm on a multiple platform environment. Since the simulator is built on multiple platform, the decision has been made to create an online cryptography learning platform which not only focuses on Trapdoor knapsack algorithm. The platform allows for customer to build other cryptographic algorithm materials on this platform.

CryptBase, an online cryptography learning platform based is created with the goal of providing a helpful visual learning experience. As a starting point, the base algorithm simulator will feature Trapdoor Knapsack, where users can learn through the step by step lessons and interact with an illustrated experience.

1.2. Introduction to Knapsack

In 1978, Ralph Merkle and Martin Hellman invented one of the earliest public key cryptosystems. It requires two keys for communication, a public key and a private key where the public key is used only for encryption and private key for decryption only.

The Merkle-Hellman system is based on Knapsack Problem as known as combinatorial optimization problem (Mathematical Term) is to find an optimal object from a finite set of objects. Given fixed size “Sack” and a set of items; each with its own weight/value. The problem arises when one tries to find the most efficient method in allocation the items into the sack. In general, there is no efficient method of finding the subset, trying all possibilities would be the best method. Knapsack for encryption are implemented as block ciphers, each block of n bits is referred to as weights

Trapdoor function is a one-way function where it is easy to compute in one direction and finding the inverse is difficult but when equipped with the knowledge of the trapdoor function the inverse can be easily calculated. A real-life example would be the padlock and key where opening the padlock would require the key. The key works like the trapdoor and the padlock as the trapdoor function. Trapdoor function is widely used in Cryptography.

Knapsack algorithm is one of the public-key cryptosystems in cryptography. It involves no expensive modular exponentiations, which makes the encryption and decryption much more efficient than discrete-logarithm-based and factorization-based cryptosystems.

For a long time, knapsack-type cryptosystems were considered to be the most attractive and the most promising due to their high speed of encryption and decryption. Many knapsack-type cryptosystems were developed in the history of knapsack public-key cryptography especially in the 1980s, and the cryptographic applications of some variants of the knapsack problem were also investigated .However, almost all additive knapsack-type cryptosystems were shown to be vulnerable to low-density subset-sum attacks ,GCD attack , simultaneous Diophantine approximation attack or orthogonal lattice attack Refer to the survey paper for the rise and fall of knapsack cryptosystems.

1.3. Problem Statement

The following table indicate about the product statement and it intention for the production.

Issue	Cryptographic Algorithm are often complicated and often misunderstood. In education and academic environment, visuals and interactive learning are proven to be a better approach.
Solution	CryptBase platform provides cryptographic learning platform presenting a step by step illustration on algorithms structure and movements. CryptBase is a web-based application which support multi-platforms accessible by mobile phones platform such as android and iOS for the ease of use and accessibility.

1.4. Product Statement Summary

For	Content creators, Education purposes
Who	Teaches Cryptographic Algorithm
In	Academia
CryptBase	Provides a means to effectively educate and manage cryptographic lessons, with the use of easy to understand animation and user-friendly graphical interface.
Unlike	Traditional static methods.

1.5. Product Features

The following table indicate about the summary of the product features.

Features	Description
User Interactive Demo	Allow users to easily interact with system using their own variable value
Animated Explanation	Step by step animated explanation on cryptographic algorithm
Topic enrolment	Course registration function before starting the lesson
Enrolment Status	Allow user to differentiation if the course has been enrolled
Topic Management	Features to add/edit the lessons as well as uploading of the files
Quiz	Attempt or set the quiz in the system

1.6. Stakeholder Type and Description

The following table indicate the different types of stakeholder that utilize the system.

Type	Description	Specification
Content creator	The owners of education materials that creates, develop and implement cryptographic algorithm materials	• Specification of requirements for the materials • Deployment of materials • Perform product testing to ensure the stability of the system
Product Developer	The one who develop and implement the product based on the user's need.	
Consumers	The one that make use of the product & it function for their needs.	• Responsible for the system usage

1.7. User type and description

The following table indicate the different types of users that utilize the system.

User Type	Description
Student	- Enrol into topic and partake in lessons - Attempt quiz - Chat for discussion
Lecturer	- Create, Update and maintain topics and lesson content in the system - Create quiz for topics - View Student learning statistic

1.8. General Requirement

The following contents indicate the general requirement of this project.

Requirement Description	Priority	Solution
Able to operate in Multiplatform	High	Can run in PC/Mac/Android/iOS platform with active connectivity to Host Server
Provide visual presentation of Algorithm	High	Using block animated visual display on step by step algorithm presentation to users

1.9. Project Goals

The main objective of the project is to provide a cryptography platform illustrating a step by step approach for each cryptography algorithm lesson. The primary goal is to promote visual learning and in return a clearer understanding for the users. The secondary goal is to interact with the users allowing the learning process to be a two-way street. Lastly, to enable different user of different platforms to access the cryptographic learning platform through their computers, laptops or mobile devices.

2. Business Context

The target audience is the academia users such as students those trying to learn cryptographic algorithms as well as for lecturers those wanted to have interactive learning platform their students.

Benefits;

1. Ease of management of content
2. Ease of delivery content to users
3. Multi-platform

Success criteria:

1. Improve efficiency in conducting lessons
2. Decreased time spent on managing a learning platform

3. Group structure

3.1. Team Member Roles

Team Member	Role
WU CHU JUN	Primary Developer & Database Designer
MARCUS TAN YONGHUA	Web UI Designer & Project Content Management
CHONG JIA HAO	System Architect & Secondary Developer
KYAW MYO AUNG	Project Coordinator & Technical Documenter

3.2. Responsibility Matrix

Task	Wu ChuJun	Marcus Tan	Chong Jia Hao	Kyaw Myo Aung
System Analyst	X	X		X
User Interface Design		X		X
Database Design	X	X	X	
System Architect			X	X
Software Programming	X	X		
Implementation	X	X	X	
Application Testing	X	X	X	X
Project Management			X	X
Project Documentation	X		X	X

4. Software Development Methodology

RUP is the chosen software development methodology. The Rational Unified Process (RUP) is an iterative software development process framework created by the Rational Software Corporation, a division of IBM since 2003. It divides the development process into four distinct phases that each involve business modelling, analysis and design, implementation, testing, and deployment.

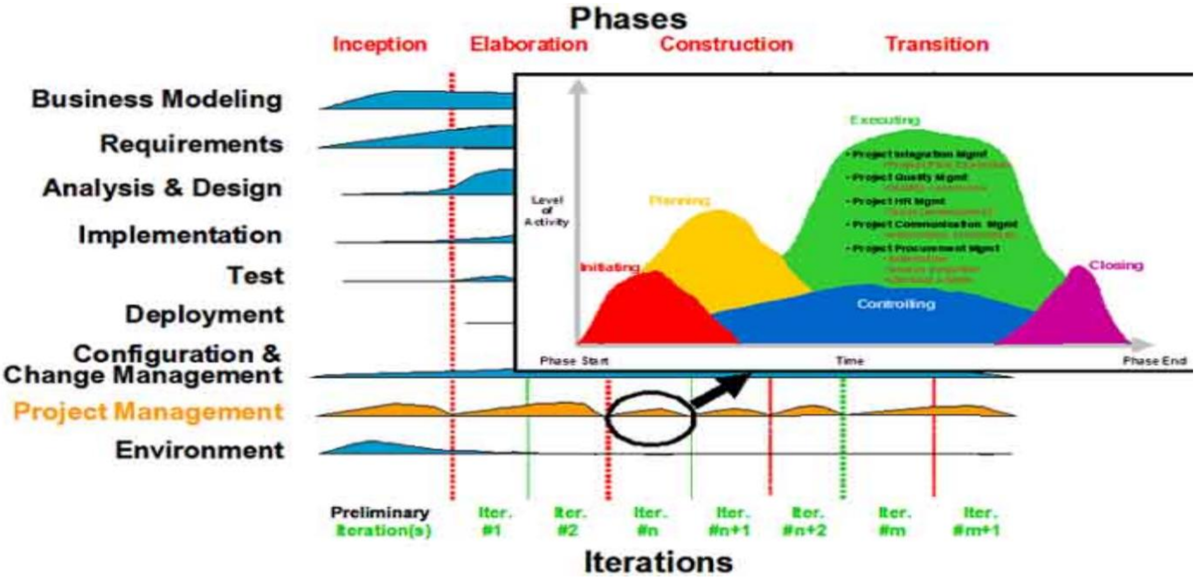
4.1. Why RUP

Rational Unified Process (RUP) is a complete methodology with an emphasis on accurate documentation. The developer will spend lesser time on repeating tasks due to reuse of components. Less time is required for integration. All the integration process must go through the software development life cycle. Change request management will help to resolve the project risks associated with client's evolving requirements.

However, RUP has some drawback such as the process of development could be complex and disorganized. And all members need to be an expert in their areas. Time and cost consuming. But still it has many advantages.

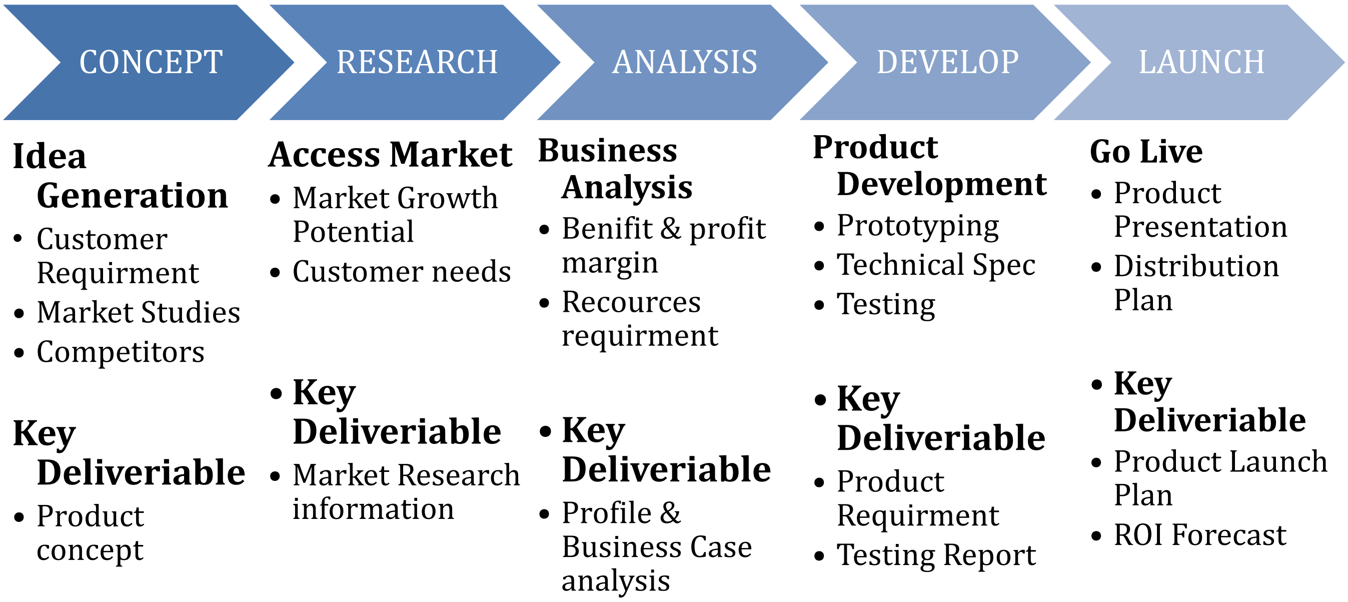
Using rational unified process (RUP) methodology for software architecture as it is complete methodology with an emphasis on accurate documentation. The developer will spend less time on repeating tasks due to reuse of components. Less time is required for integration. All the integration process has to go through the software development life cycle.

Change request management will help to resolve the project risks associated with client's evolving requirements. Below is the basic software architecture for RUP methodology



4.2. Project Management Methodology

Below process chart indicate the process management flow in this project.



CONCEPT

Idea Generation

- Customer Requirment
- Market Studies
- Competitors

Key Deliveriable

- Product concept

RESEARCH

Access Market

- Market Growth Potential
- Customer needs
- **Key Deliveriable**
- Market Research information

ANALYSIS

Business Analysis

- Benifit & profit margin
- Recources requirment
- **Key Deliveriable**
- Profile & Business Case analysis

DEVELOP

Product Development

- Prototyping
- Technical Spec
- Testing
- **Key Deliveriable**
- Product Requirment
- Testing Report

LAUNCH

Go Live

- Product Presentation
- Distribution Plan
- **Key Deliveriable**
- Product Launch Plan
- ROI Forecast

5. Project timeline

5.1. Phase 1 Project timeline

Project phase 1, it is on information gathering, market analysis, understanding users need & project proposal. The detail planning and activity list for phase 1 can be found in below table.

Event	Duration	Description
Project Briefing & role allocation	3 days	Discussion on overview of the project and role/responsibility allocation
Project Kick-Off Meeting	1 days	Verification of project nature with supervisor
Market Research	5 days	Understanding market research and user needs
Project Proposal Preparation	7 days	Draft plan of project proposal documentation
Requirement Gathering	3 days	Detail requirement gathering of product and competitors' products
Web UI Design Research	3 days	UI design brainstorming and research
Scope and Goal Setting	2 days	Setting Project goals and scope of works
Gathering Functional Features	2 days	Detail information of functional feature to be included in the product
Use Case diagram	4 days	Use case diagram of how use will interact with the system
Database ERD diagram Design	4 days	Entity relationship diagram
Sequence Diagram	4 days	Software workflow and sequence diagram
Web UI Design Finalization	3 days	UI design finalization and choosing the web template
Web content Management	8 days	Content of UI for the website
Risk Management	2 days	Risk measurement and management
Status and Tracking	1 days	Reviewing overall project status and activity tracking
Installation of Host VM and configuration	2 days	Beginning of implementation to install host server
Web UI Installation	5 days	Deployment of chosen web template
Basic MySQL Database Setup	3 days	MySQL database installation on host VM
Implementation of Basic Functionalities	14 days	Beginning of functional feature implementation
Prototype Demo and Presentation Session	2 days	Reviewing the project prototype for phase1 presentation

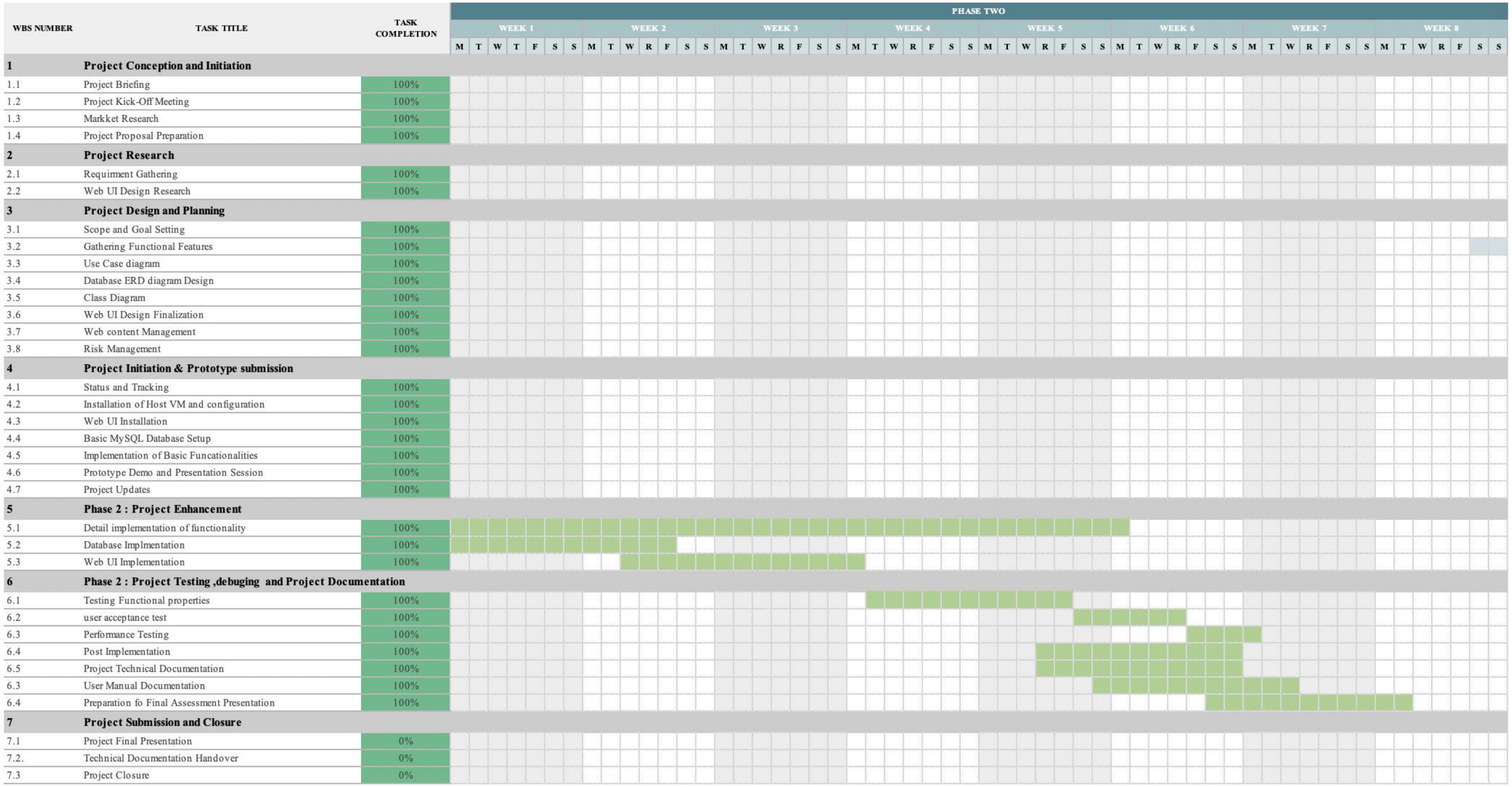
WBS NUMBER	TASK TITLE	TASK COMPLETION	PHASE ONE																																																												
			WEEK 1							WEEK 2							WEEK 3							WEEK 4							WEEK 5							WEEK 6							WEEK 7							WEEK 8							WEEK 9						
			M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S	M	T	W	R	F	S	S
1	**Project Conception and Initiation**																																																													
1.1	Project Briefing	100%							🟦	🟦	🟦																																																			
1.2	Project Kick-Off Meeting	100%										🟦																																																		
1.3	Markket Research	100%										🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦																																											
1.4	Project Proposal Preparation	100%															🟦	🟦	🟦	🟦																																										
2	**Project Research**																																																													
2.1	Requirment Gathering	100%																🟦	🟦	🟦																																										
2.2	Web UI Design Research	100%																🟦	🟦	🟦																																										
3	**Project Design and Planning**																																																												
3.1	Scope and Goal Setting	100%																			🟦	🟦																																								
3.2	Gathering Functional Features	100%																				🟦	🟦																																							
3.3	Use Case diagram	100%																					🟦	🟦	🟦	🟦																																				
3.4	Database ERD diagram Design	100%																							🟦	🟦	🟦	🟦																																		
3.5	Class Diagram	100%																											🟦	🟦	🟦	🟦																																
3.6	Web UI Design Finalization	100%																															🟦	🟦	🟦																													
3.7	Web content Management	100%																														🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦																										
3.8	Risk Management	100%																																				🟦	🟦																										
4	**Project Initiation & Prototype submission**																																																													
4.1	Status and Tracking	100%																																						🟦																									
4.2	Installation of Host VM and configuration	100%																																						🟦	🟦																								
4.3	Web UI Installation	100%																																								🟦	🟦																						
4.4	Basic MySQL Database Setup	100%																																										🟦	🟦	🟦	🟦	🟦	🟦																
4.5	Implementation of Basic Funcationalities	100%																																													🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦			
4.6	Prototype Demo and Presentation Session	100%																																																												🟦		
4.7	Project Updates	100%																																																												🟦	🟦	🟦
5	**Phase 2 : Project Enhancement**																																																													
5.1	Detail implementation of functionality	100%																																													🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
5.2	Database Implmentation	100%																																																												🟩	🟩	🟩
5.3	Web UI Implementation	100%																																																														
6	**Phase 2 : Project Testing ,debuging and Project Documentation**																																																													
6.1	Testing Functional properties	100%																																																													
6.2	user acceptance test	100%																																																													
6.3	Performance Testing	100%																																																													
6.4	Post Implementation	100%																																																													
6.5	Project Technical Documentation	100%																																																													
6.3	User Manual Documentation	100%																																																													
6.4	Preparation fo Final Assessment Presentation	100%																																																													
7	**Project Submission and Closure**																																																													
7.1	Project Final Presentation	0%																																																													
7.2.	Technical Documentation Handover	0%																																																													
7.3	Project Closure	0%																																																													

5.2. Phase 2 Project timeline

Project phase 2, focus is placed on product implementation, functional feature testing and preparing of project documentation.

The detail planning and activity list for phase 2 can be found in below table.

Event	Duration	Description
Detail implementation of functionality	6 weeks	Development of propose function features
Database Implementation	2 weeks	Populating of data tables and detail implementation
Web UI Implementation	2 weeks	Updating web content and web UI fine tuning
Project debugging	7 days	Program debugging and troubleshooting on encounter errors
Testing Functional properties	7 days	Software functional testing
User acceptance test	3 days	UAT test cases and demo on user verification on system
Performance Testing	2 days	System reliability testing
Post Implementation	7 days	Minor finetuning on system and hotfixes
Project Technical Documentation	4 days	Preparation of technical documentation such as Deployment document
User Manual Documentation	4 days	User guide document preparation
Project Final Presentation	1 days	Preparation of final submission such as product video and other documentation



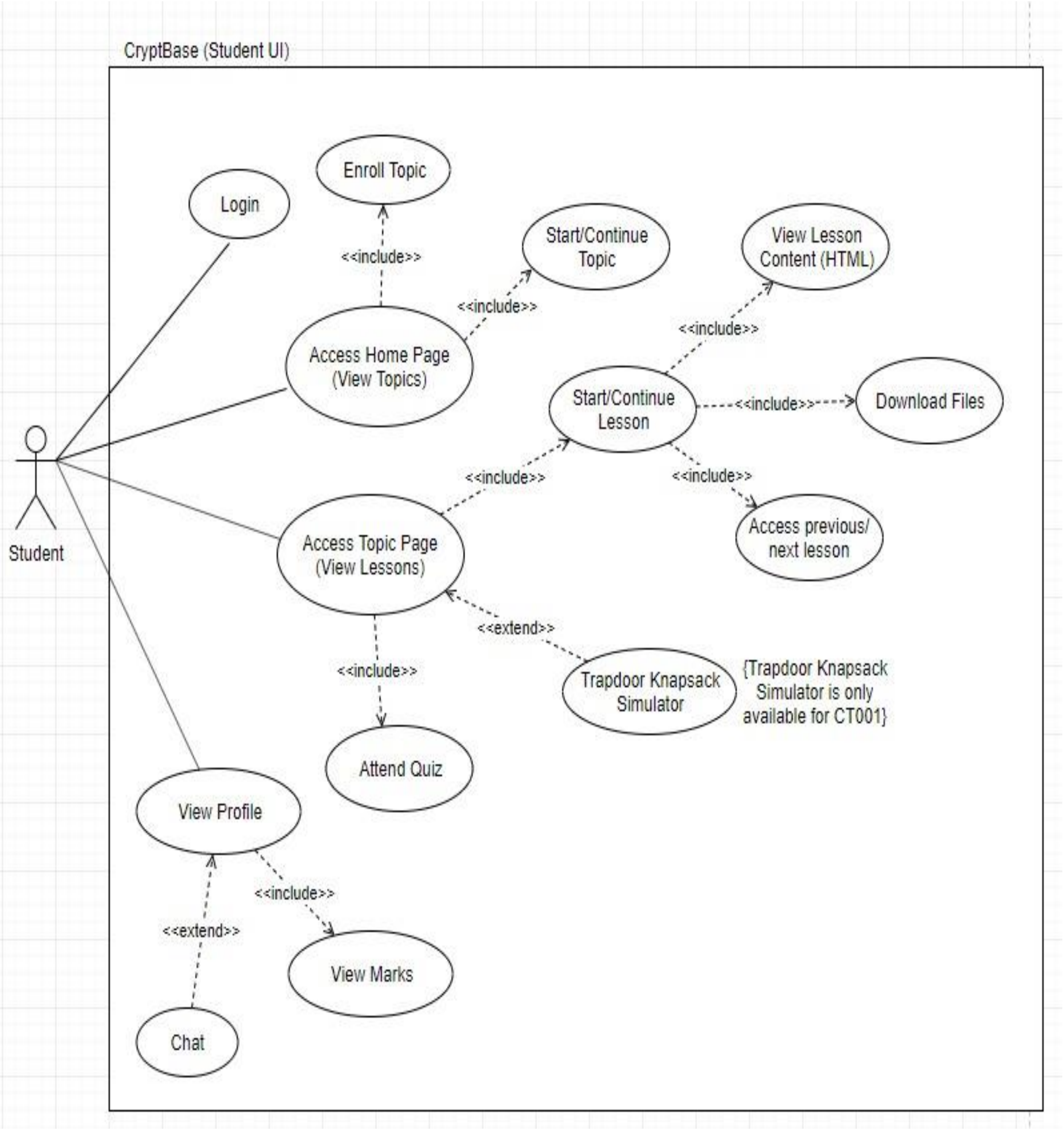
WBS NUMBER	TASK TITLE	TASK COMPLETION
1	**Project Conception and Initiation**	
1.1	Project Briefing	100%
1.2	Project Kick-Off Meeting	100%
1.3	Markket Research	100%
1.4	Project Proposal Preparation	100%
2	**Project Research**	
2.1	Requirment Gathering	100%
2.2	Web UI Design Research	100%
3	**Project Design and Planning**	
3.1	Scope and Goal Setting	100%
3.2	Gathering Functional Features	100%
3.3	Use Case diagram	100%
3.4	Database ERD diagram Design	100%
3.5	Class Diagram	100%
3.6	Web UI Design Finalization	100%
3.7	Web content Management	100%
3.8	Risk Management	100%
4	**Project Initiation & Prototype submission**	
4.1	Status and Tracking	100%
4.2	Installation of Host VM and configuration	100%
4.3	Web UI Installation	100%
4.4	Basic MySQL Database Setup	100%
4.5	Implementation of Basic Funcationalities	100%
4.6	Prototype Demo and Presentation Session	100%
4.7	Project Updates	100%
5	**Phase 2 : Project Enhancement**	
5.1	Detail implementation of functionality	100%
5.2	Database Implmentation	100%
5.3	Web UI Implementation	100%
6	**Phase 2 : Project Testing ,debuging and Project Documentation**	
6.1	Testing Functional properties	100%
6.2	user acceptance test	100%
6.3	Performance Testing	100%
6.4	Post Implementation	100%
6.5	Project Technical Documentation	100%
6.3	User Manual Documentation	100%
6.4	Preparation fo Final Assessment Presentation	100%
7	**Project Submission and Closure**	
7.1	Project Final Presentation	0%
7.2.	Technical Documentation Handover	0%
7.3	Project Closure	0%

<The full project timeline file can be review in Appendix A >

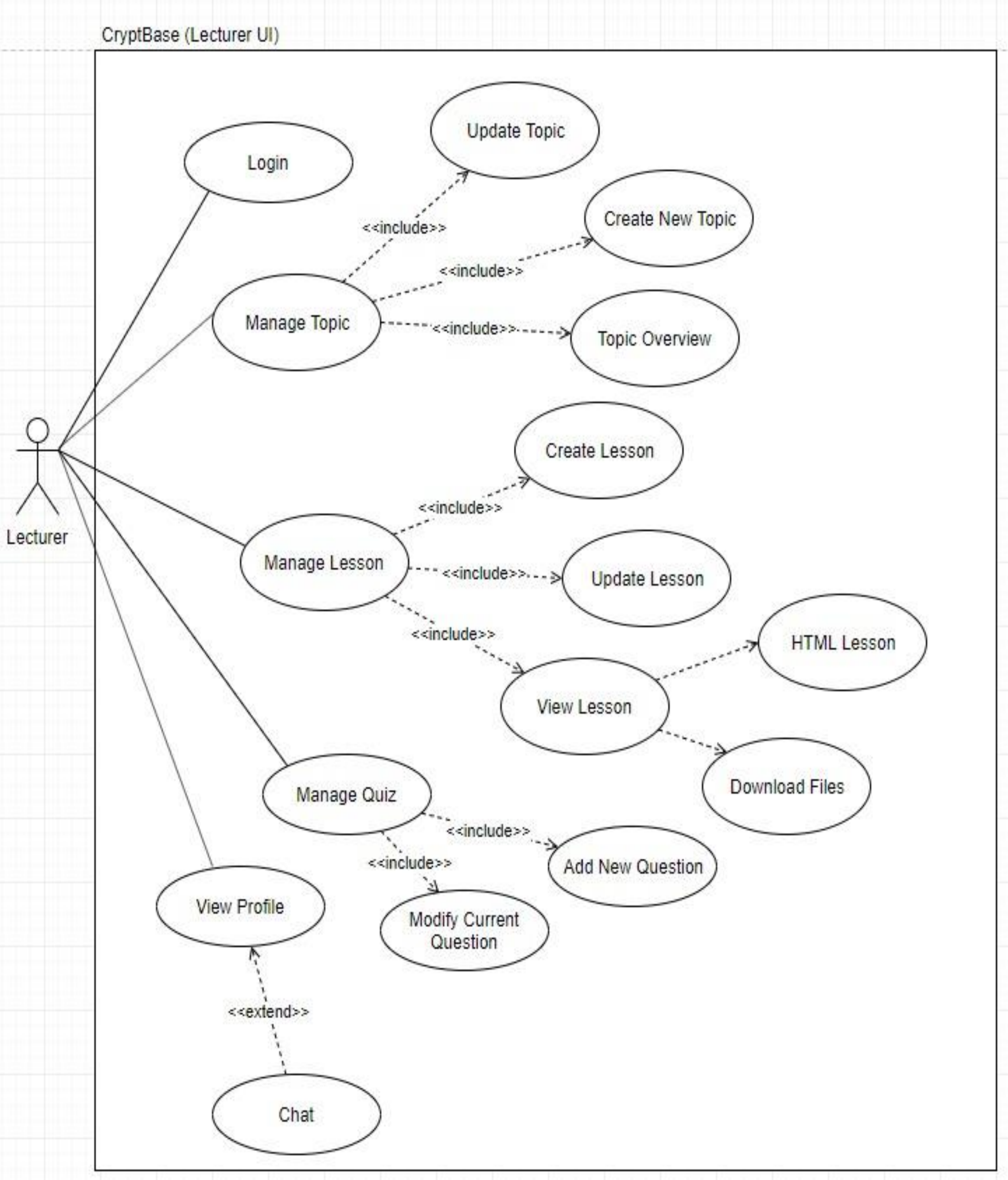
6. Use Cases

The use case diagram illustrates how users will interact with the CryptBase System. The following use case diagram indicate what are the functions that will be implemented and included in this CryptBase Platform.

6.1. Use case diagram for student

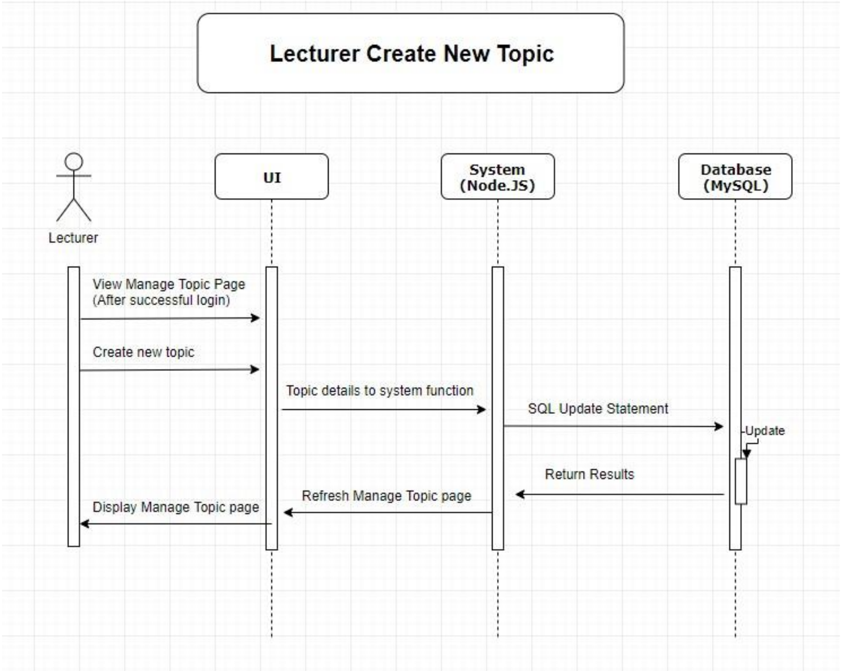


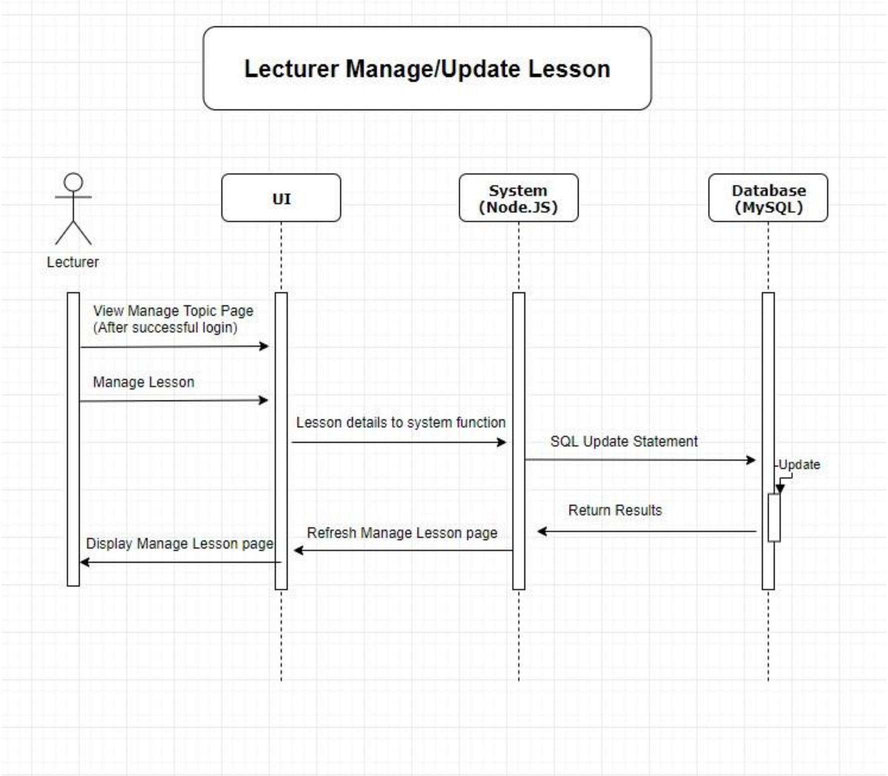
6.2. Use case diagram for lecturer

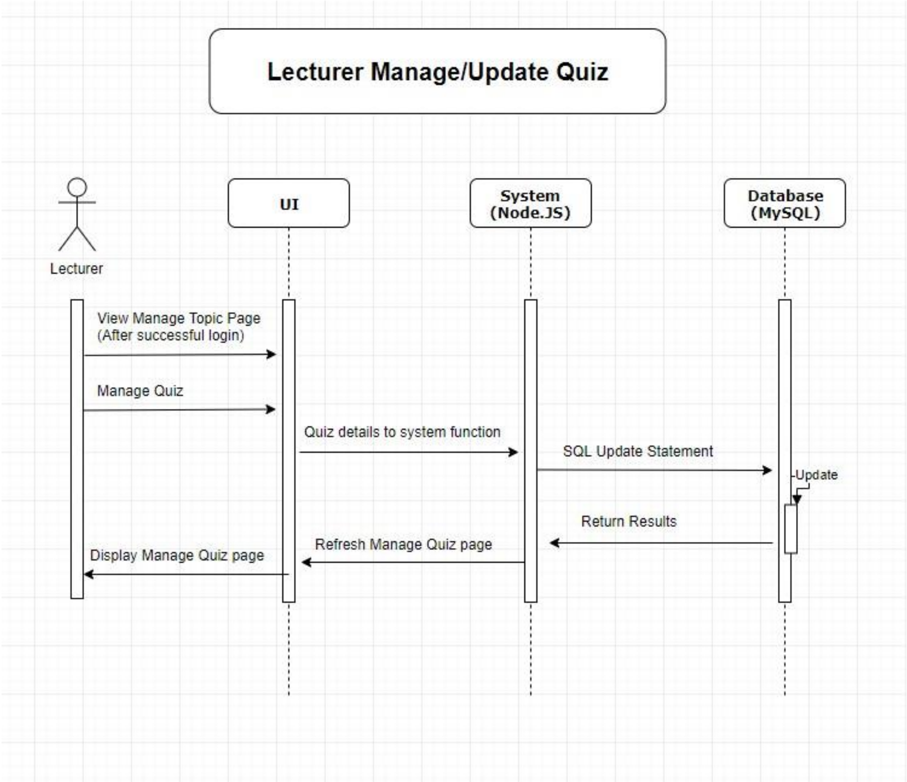


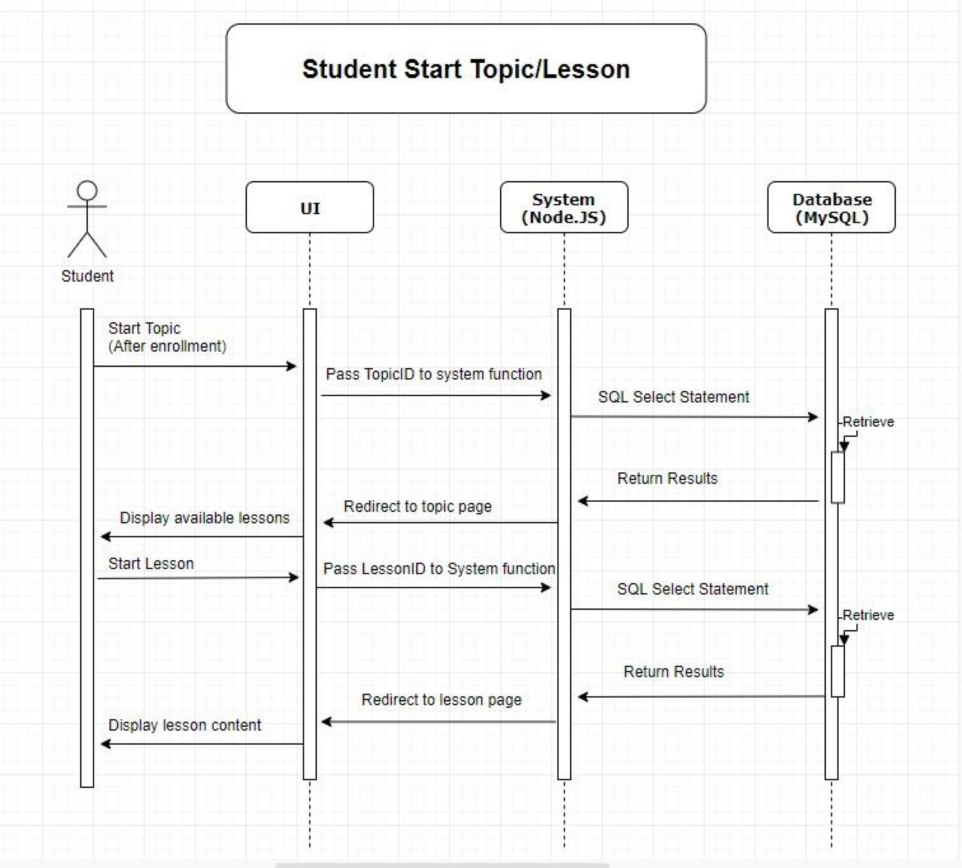
7. Sequence diagram

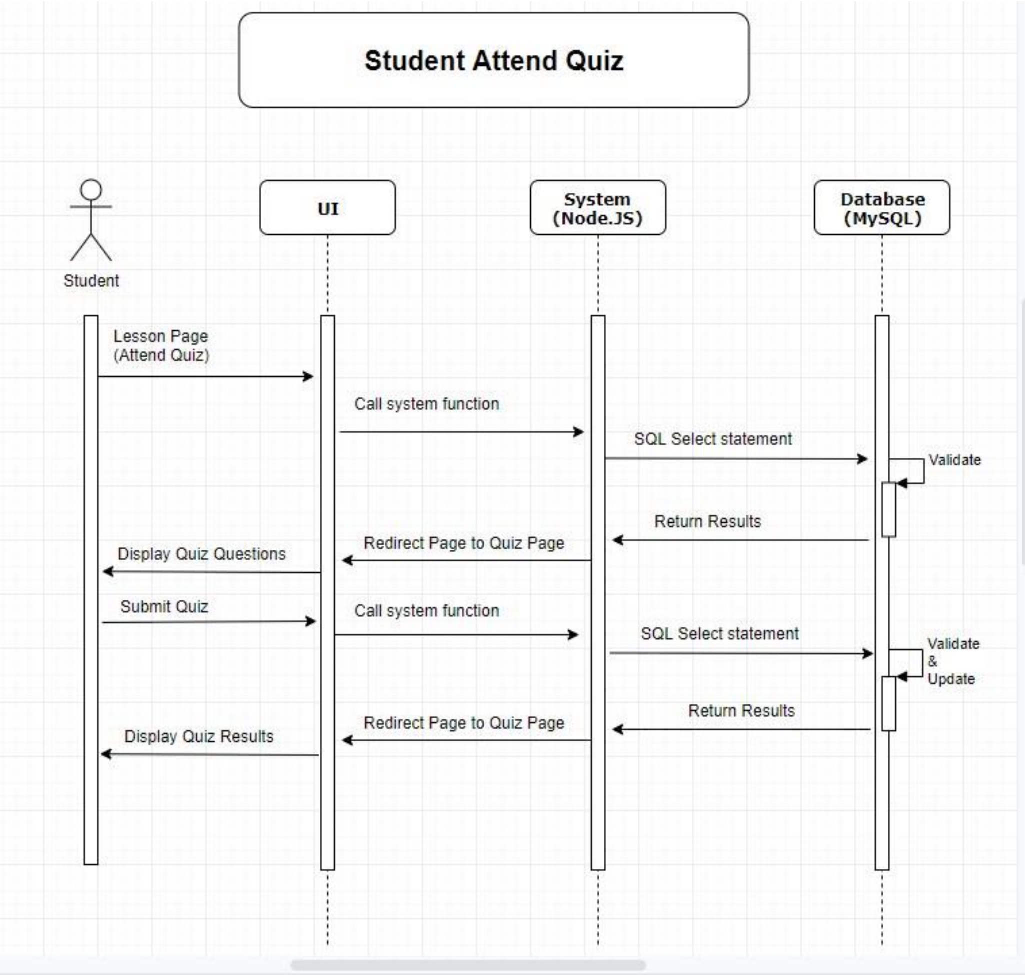
The sequence diagram indicates how one objects interact with others in time. In this project, there are various types of users interacting with system such as student and lecturer as shown below.

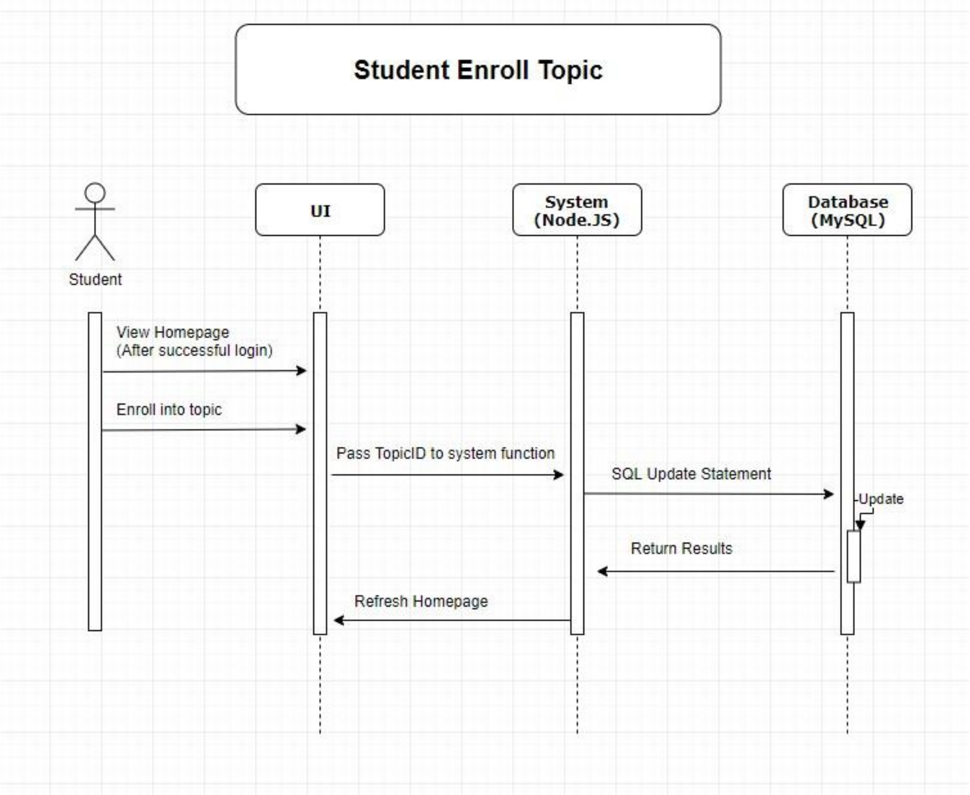

Lecturer Create New Topic
Lecturer
UI
System (Node.JS)
Database (MySQL)
View Manage Topic Page (After successful login)
Create new topic
Topic details to system function
SQL Update Statement
Update
Return Results
Refresh Manage Topic page
Display Manage Topic page

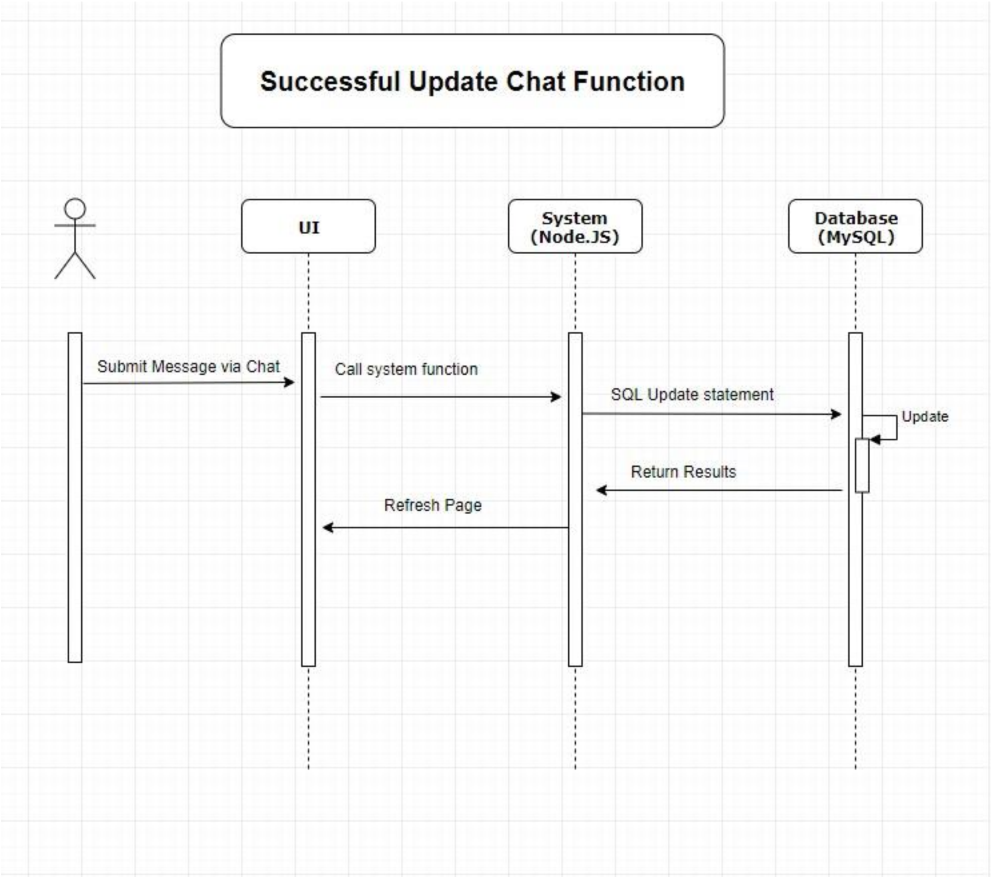

Lecturer Manage/Update Lesson
Lecturer
UI
System (Node.JS)
Database (MySQL)
View Manage Topic Page (After successful login)
Manage Lesson
Lesson details to system function
SQL Update Statement
Update
Return Results
Refresh Manage Lesson page
Display Manage Lesson page

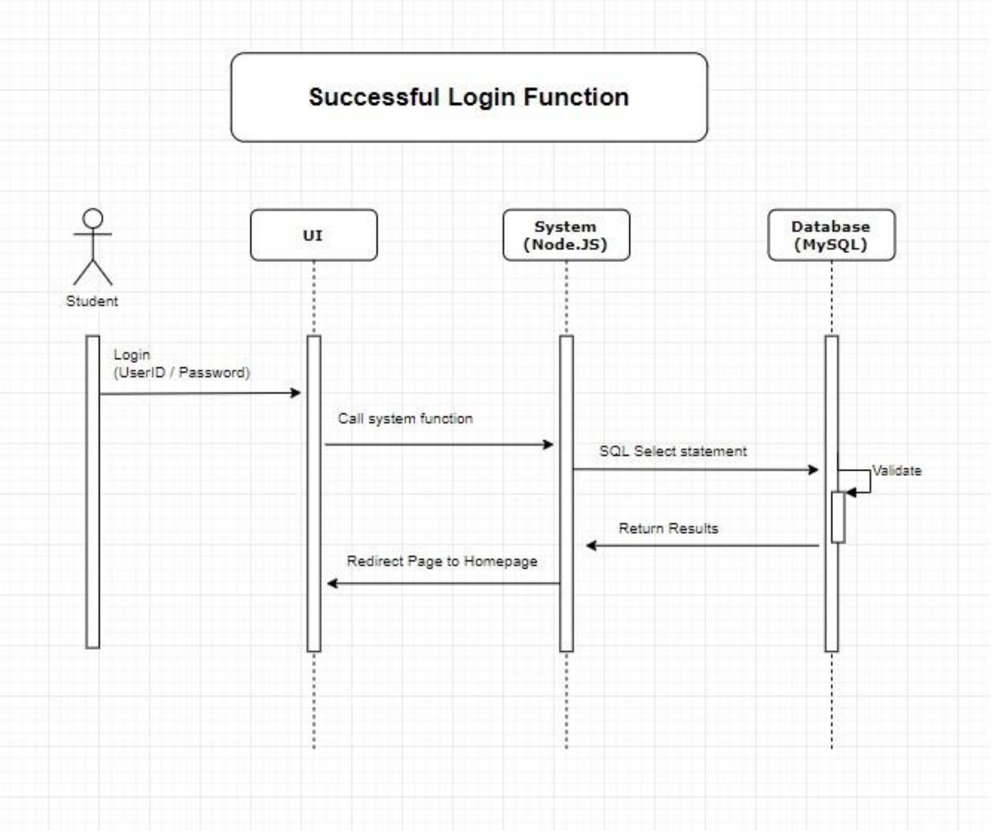

Lecturer Manage/Update Quiz
Lecturer
UI
System (Node.JS)
Database (MySQL)
View Manage Topic Page (After successful login)
Manage Quiz
Quiz details to system function
SQL Update Statement
Update
Return Results
Refresh Manage Quiz page
Display Manage Quiz page


Student Start Topic/Lesson
Student
UI
System (Node.JS)
Database (MySQL)
Start Topic (After enrollment)
Pass TopicID to system function
SQL Select Statement
Retrieve
Return Results
Redirect to topic page
Display available lessons
Start Lesson
Pass LessonID to System function
SQL Select Statement
Retrieve
Return Results
Redirect to lesson page
Display lesson content


Student Attend Quiz
Student
UI
System (Node.JS)
Database (MySQL)
Lesson Page (Attend Quiz)
Call system function
SQL Select statement
Validate
Return Results
Redirect Page to Quiz Page
Display Quiz Questions
Submit Quiz
Call system function
SQL Select statement
Validate & Update
Return Results
Redirect Page to Quiz Page
Display Quiz Results

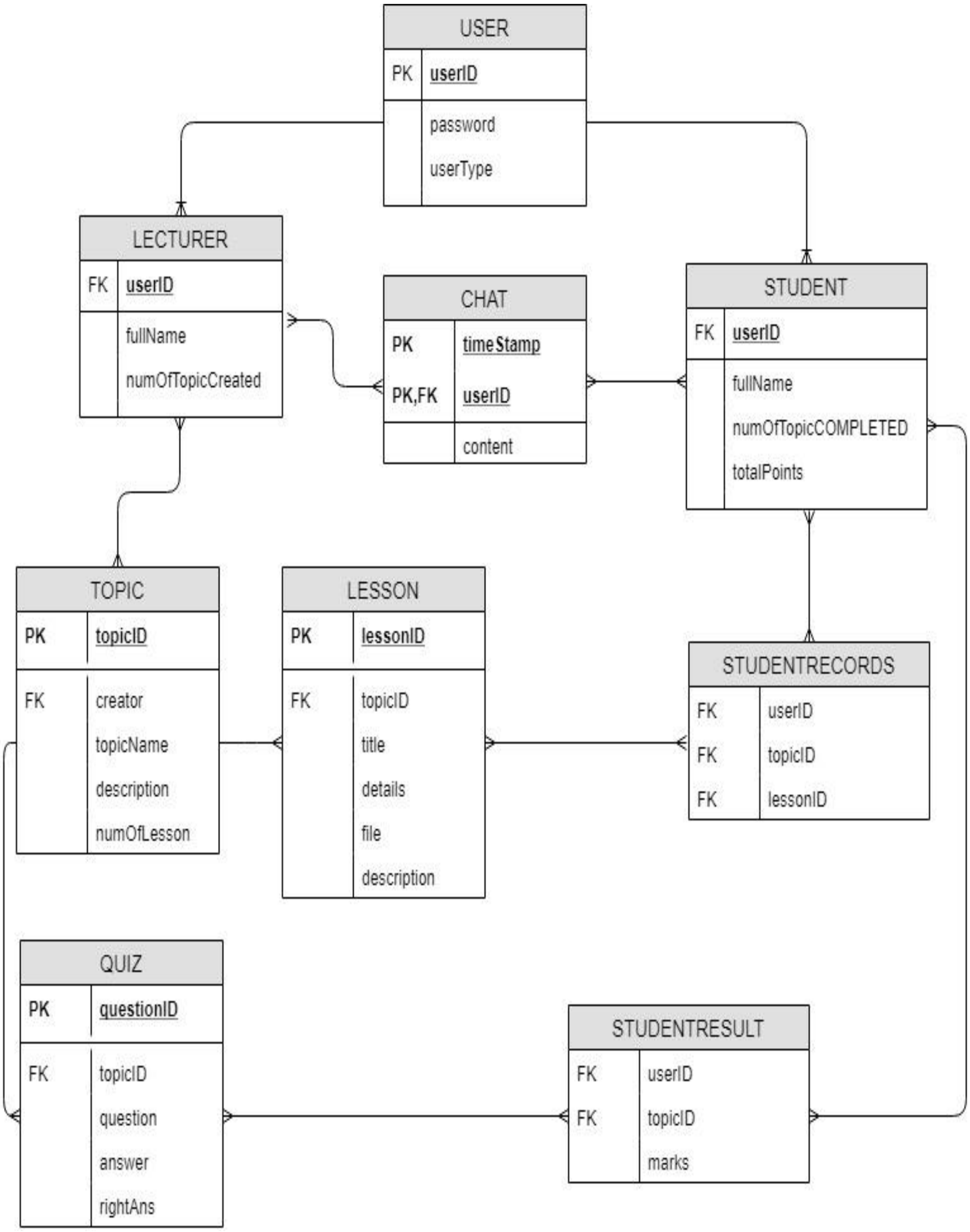

Student Enroll Topic
Student
UI
System (Node.JS)
Database (MySQL)
View Homepage (After successful login)
Enroll into topic
Pass TopicID to system function
SQL Update Statement
Update
Return Results
Refresh Homepage


Successful Update Chat Function
UI
System (Node.JS)
Database (MySQL)
Submit Message via Chat
Call system function
SQL Update statement
Update
Return Results
Refresh Page


Successful Login Function
Student
UI
System (Node.JS)
Database (MySQL)
Login (UserID / Password)
Call system function
SQL Select statement
Validate
Return Results
Redirect Page to Homepage

8. Entity Relationship Diagram (ERD)

CryptBase Platform is using a MySQL database to store users and systems related information. The following is the entity relationship diagram (ERD) of CryptBase Database design and its attributes



9. Assumption & Risk Assessment

9.1. Assumptions

9.1.1. Design assumptions

Mobile UI design will be customized based on standard model of phone screen size

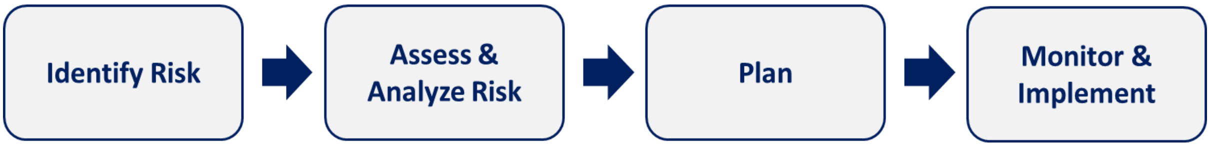
9.1.2. Implementation assumptions

Even Though CryptBase is web-based crypto learning application, for a start it will mainly focus on knapsack algorithm. New feature can be add-on in the future

CryptBase weblink will be hosted privately and will not be available to public due to security reason of the project's contents

9.2. Risk analysis

Identify key risk factors (with regards to technology, market, finance, regulatory, stakeholders, management etc.) and describe planned measures to anticipate/mitigate such risks.



9.2.1. Risks Assessment

Description of Risks	**Level of Likelihood (LOW/MED/HIGH)**	**Propose risk-mitigation Measure**
Lack of Redundant hosting servers /Secondary Database	MED	*Suggest having redundant system in future*
Limited programming knowledge	MED	• Spend more time to understand the language • Seek mentor advise
Limited Implementation Timeline in Phase 2	HIGH	Plan on phase 1

10. Architecture

10.1. Framework and Software used

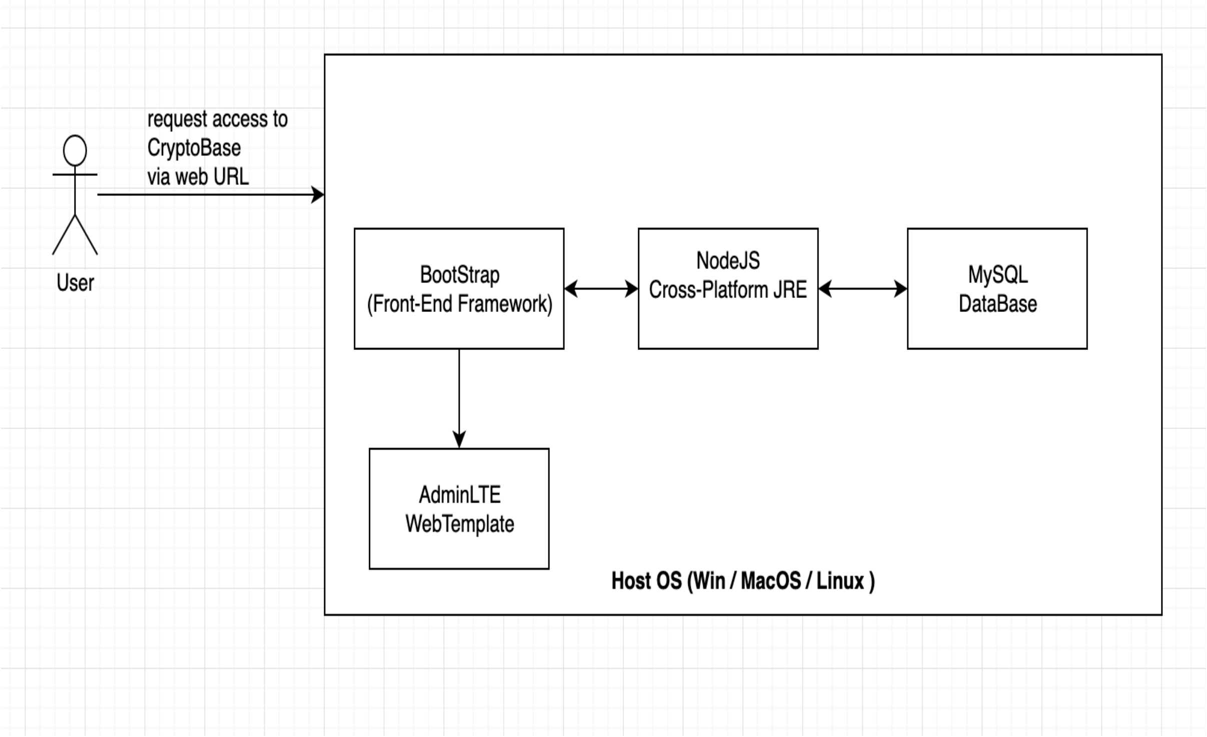
CryptBase is a web-based service. User can access CryptBase via a browser from various platforms. All components are sitting on top of ubuntu environment. It uses a Many-to-One architectural design.

CryptBase Platform include multiple components such as

- AdminLTE, a web template using Bootstraps (front-end framework)
- NodeJS, as cross-platform Java runtime environment
- MySQL Database

The use of NodeJS allows CryptBase to run on any common operating system such as Win/MacOS/Linux.

The following is a high-level overview software architecture of components in CryptBase which users will be accessing.



10.2. Framework

10.2.1. NodeJS

Node.js is JavaScript run-time environment which executes JavaScript code outside of a browser.Node.js uses asynchronous programming which provide common task for a web server can be to open a file on the server and return the content to the client. It is an open-source, supported on cross-platform

10.2.2. Bootstrap

Bootstrap is an open-source front-end framework which provide faster and easier web development. It contains HTML and CSS based design templates for typography, forms, buttons, tables, navigation, modals, image carousels and many other, as well as optional JavaScript plugins.

10.3. Software

10.3.1. MySQL Database

MySQL, an open-source relational database management system, will be used to manage the database contents of the system. MySQL is free software that based on Structured Query Language (SQL) which support multiple platform including Linux and windows system.

10.4. Collaboration Tools

10.4.1. Github

GitHub provide a web-based version control hosting service. It hosts mostly the computer coding. It is an open-source platform which offers all of the distributed version control and source code management functionality of Git as well as adding its own features.

10.5. OS & Development Environment

10.5.1. Ubuntu Linux Operating System

Ubuntu is the free distributed version Linux operating system which a stable, predictable, manageable and reproducible platform-based Debian. In this project, Ubuntu OS will be hosting all the application such as MySQL, Bootstrap, Node JS and so on.

10.5.2. NetBeans

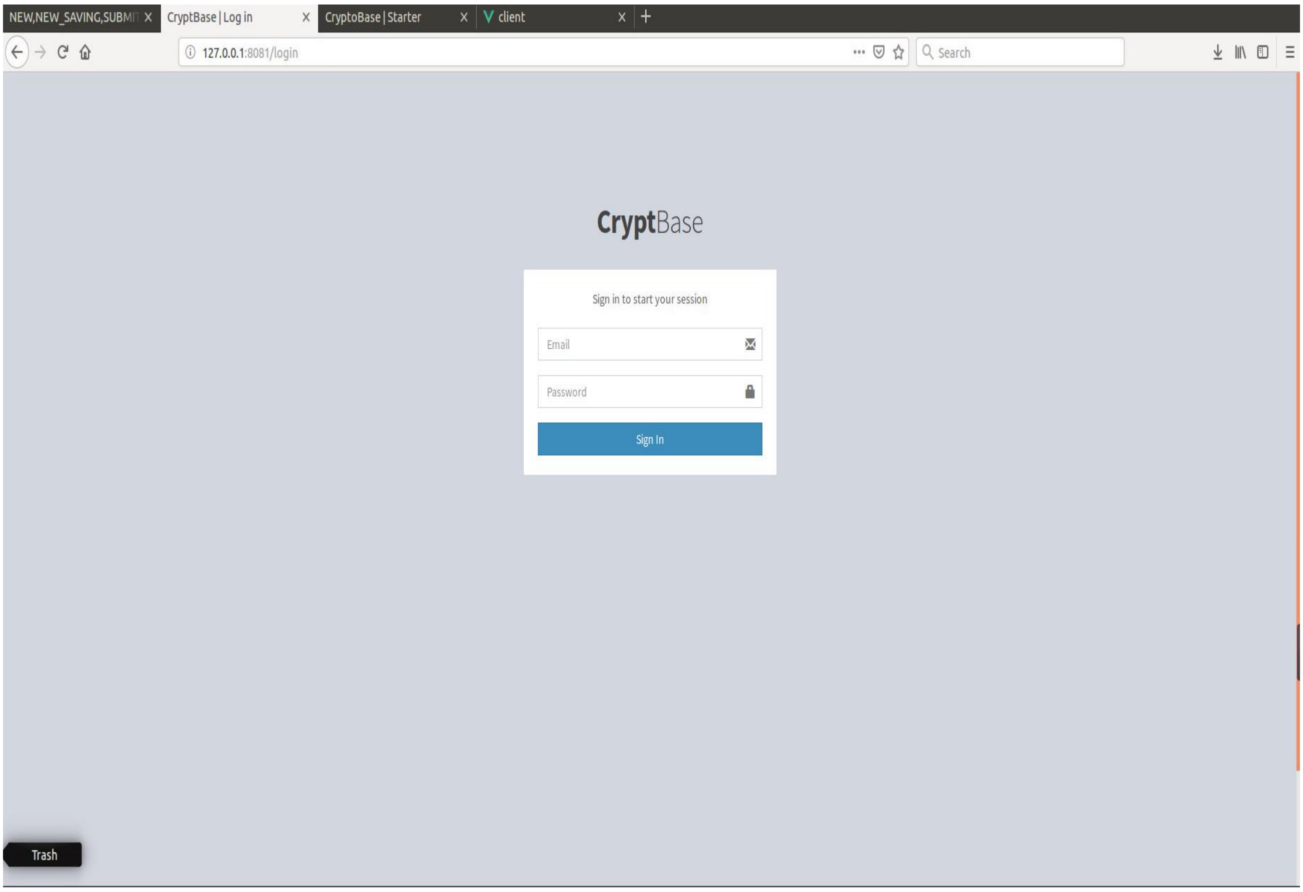
NetBeans is the software integration development environment (IDE) that used to compile and execute the user's implemented program. NetBeans is a freeware that runs on multiple platforms such as windows, Linux and MacOS. It is very user friendly and easy to use for various programming languages.

11. Functional and Non-Functional Features

11.1. Functional Features

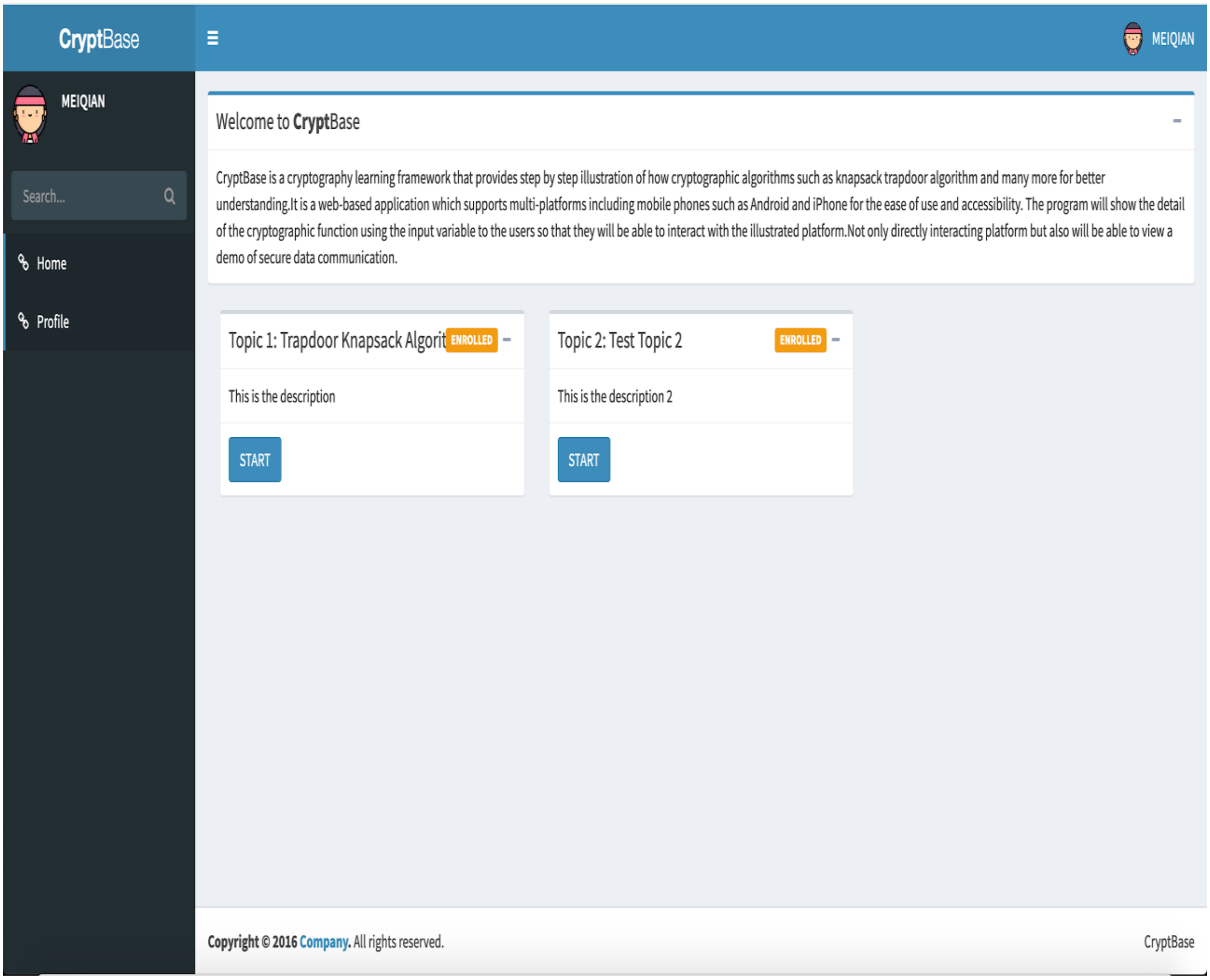
11.1.1. SECURE LOGIN using username & password

CryptBase system provides secure login using username and password. Users are validated before obtaining access to the system and their learning profile without the correct credentials and authority. The login info such as userID and password are all store in secure database system.



11.1.2. Student Homepage

Once student users are validated, they will be redirected to the homepage where it would display a welcome message and a list of various topics created by the lecturers. Other feature such as viewing profile and chat are included in the profile page as shown below:



Welcome to **Crypt**Base

CryptBase is a cryptography learning framework that provides step by step illustration of how cryptographic algorithms such as knapsack trapdoor algorithm and many more for better understanding.It is a web-based application which supports multi-platforms including mobile phones such as Android and iPhone for the ease of use and accessibility. The program will show the detail of the cryptographic function using the input variable to the users so that they will be able to interact with the illustrated platform.Not only directly interacting platform but also will be able to view a demo of secure data communication.

Topic 1: Trapdoor Knapsack Algorit ENROLLED

This is the description

START

Topic 2: Test Topic 2 ENROLLED

This is the description 2

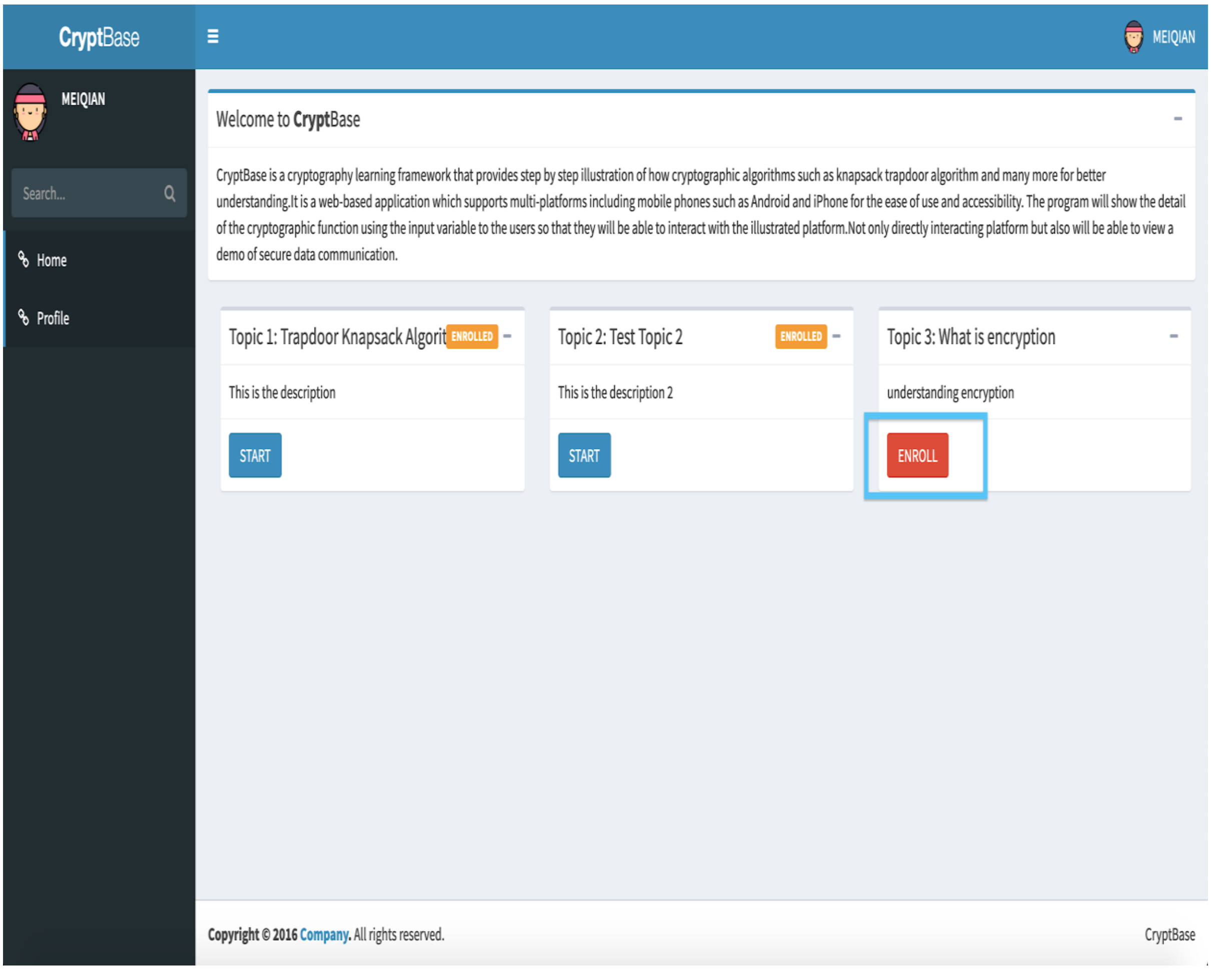
START

Copyright © 2016 Company. All rights reserved.

CryptBase

11.1.3. Topic Enrolment

Upon a successful login, user is required to enrol themselves into topics before proceeding into the topic lessons. This is done simply by clicking the enrolment button as shown below:



Welcome to **Crypt**Base

CryptBase is a cryptography learning framework that provides step by step illustration of how cryptographic algorithms such as knapsack trapdoor algorithm and many more for better understanding.It is a web-based application which supports multi-platforms including mobile phones such as Android and iPhone for the ease of use and accessibility. The program will show the detail of the cryptographic function using the input variable to the users so that they will be able to interact with the illustrated platform.Not only directly interacting platform but also will be able to view a demo of secure data communication.

Topic 1: Trapdoor Knapsack Algorit ENROLLED

This is the description

START

Topic 2: Test Topic 2 ENROLLED

This is the description 2

START

Topic 3: What is encryption

understanding encryption

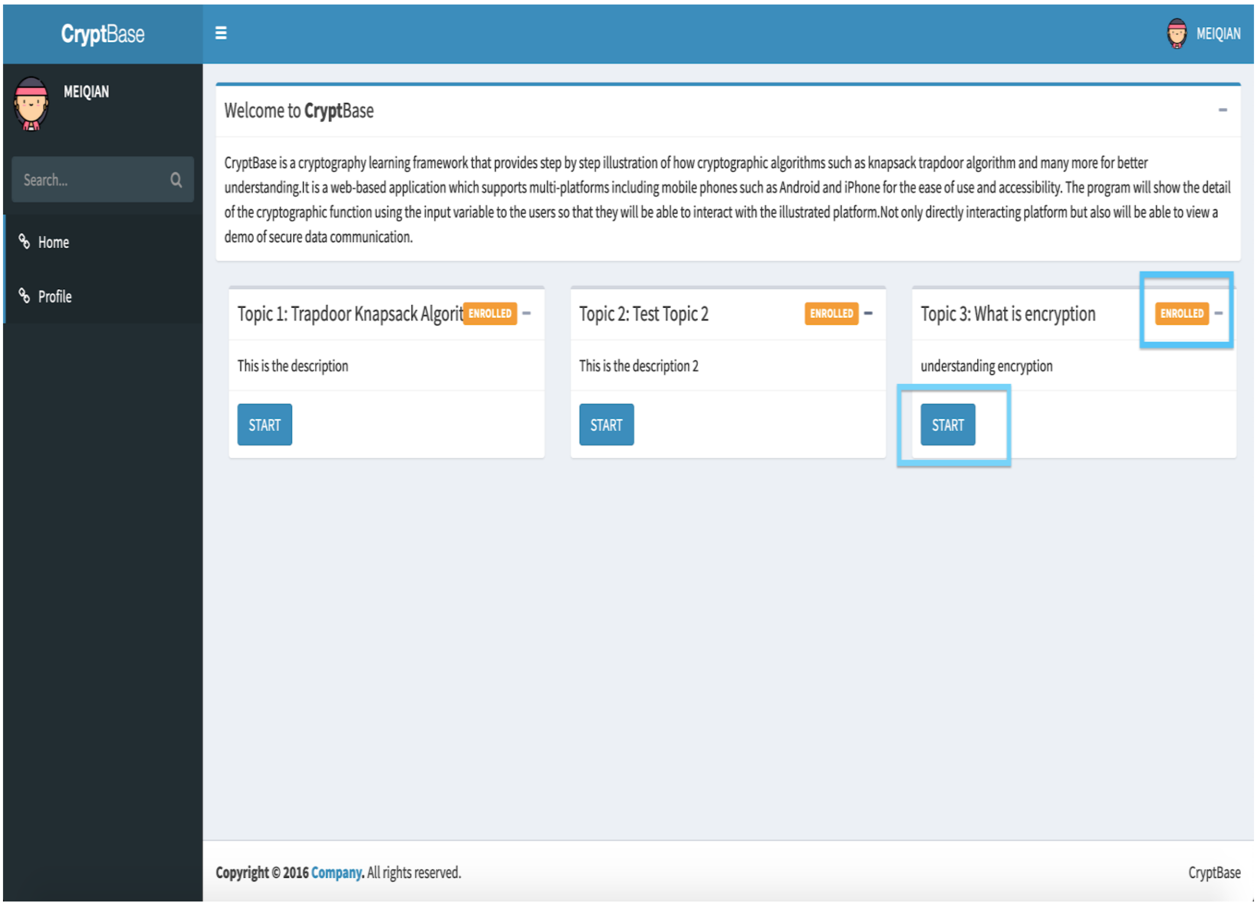
ENROLL

Copyright © 2016 Company. All rights reserved.

CryptBase

11.1.4. Enrolment Status

In an instance where the topic is enrolled by a student, the enrolment status will be displayed at the topic as shown below:



Welcome to **Crypt**Base

CryptBase is a cryptography learning framework that provides step by step illustration of how cryptographic algorithms such as knapsack trapdoor algorithm and many more for better understanding.It is a web-based application which supports multi-platforms including mobile phones such as Android and iPhone for the ease of use and accessibility. The program will show the detail of the cryptographic function using the input variable to the users so that they will be able to interact with the illustrated platform.Not only directly interacting platform but also will be able to view a demo of secure data communication.

Topic 1: Trapdoor Knapsack Algorit ENROLLED

This is the description

Topic 2: Test Topic 2 ENROLLED

This is the description 2

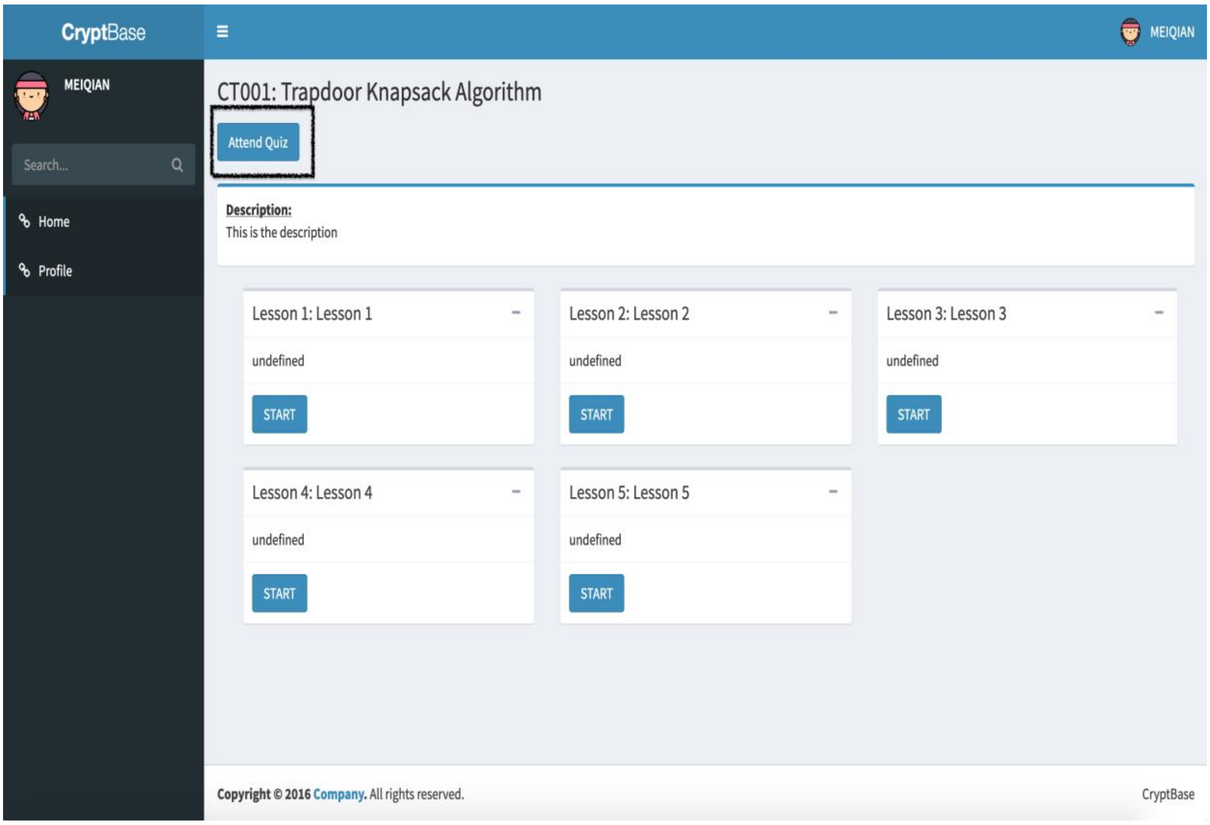
Topic 3: What is encryption ENROLLED

understanding encryption

Copyright © 2016 Company. All rights reserved.

11.1.5. Student Knowledge Test Quiz

Students are encouraged to attend the quiz for each topic as shown below:



CT001: Trapdoor Knapsack Algorithm

Description:
This is the description

Lesson 1: Lesson 1
undefined

Lesson 2: Lesson 2
undefined

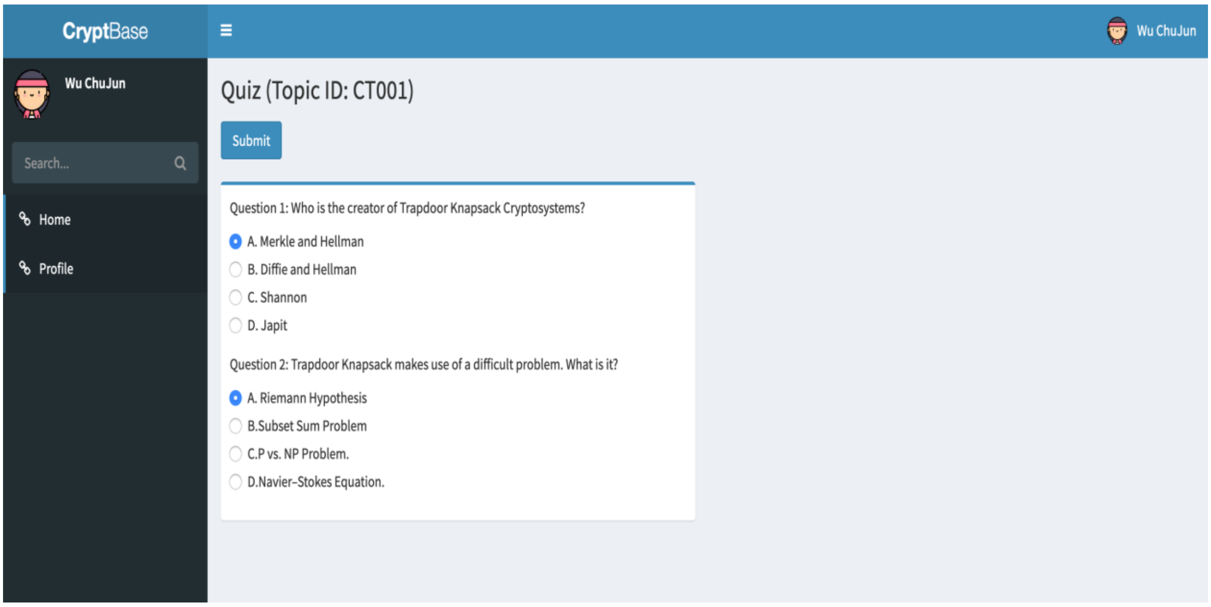
Lesson 3: Lesson 3
undefined

Lesson 4: Lesson 4
undefined

Lesson 5: Lesson 5
undefined

Copyright © 2016 Company. All rights reserved.

The following screenshot shown that snapshot of the quiz feature



Quiz (Topic ID: CT001)

Question 1: Who is the creator of Trapdoor Knapsack Cryptosystems?

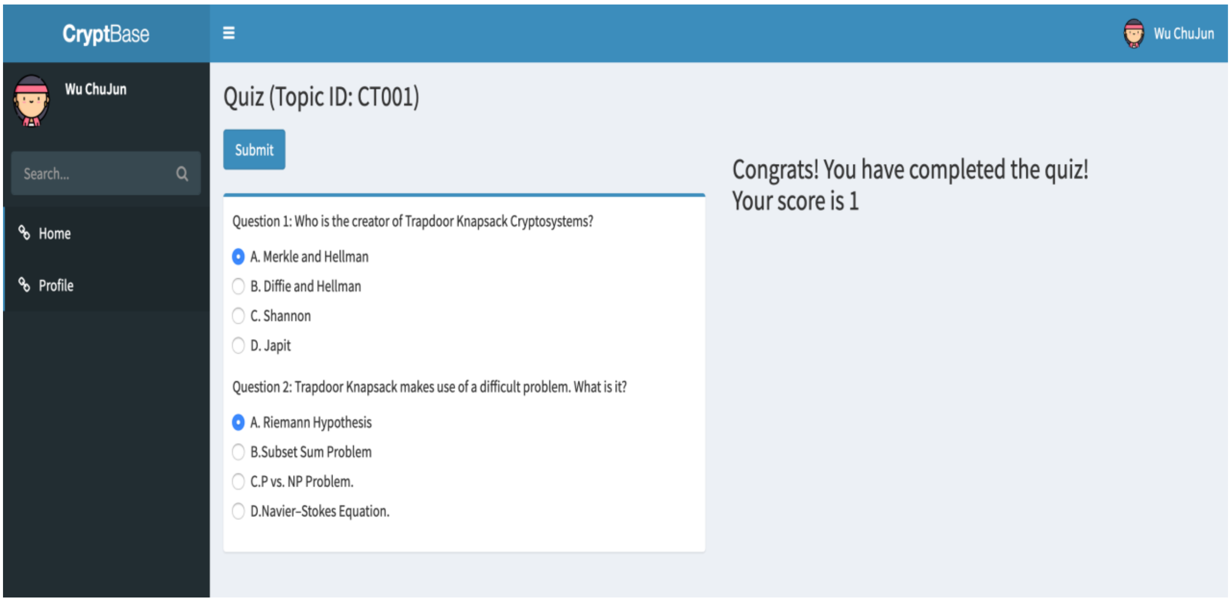
● A. Merkle and Hellman
○ B. Diffie and Hellman
○ C. Shannon
○ D. Japit

Question 2: Trapdoor Knapsack makes use of a difficult problem. What is it?

● A. Riemann Hypothesis
○ B.Subset Sum Problem
○ C.P vs. NP Problem.
○ D.Navier-Stokes Equation.

11.1.6. Student Learning Point

Students are awarded for learning points upon completion of each topic. And also, by scoring the correct answer in the quiz as shown below:



Quiz (Topic ID: CT001)

Question 1: Who is the creator of Trapdoor Knapsack Cryptosystems?

● A. Merkle and Hellman
○ B. Diffie and Hellman
○ C. Shannon
○ D. Japit

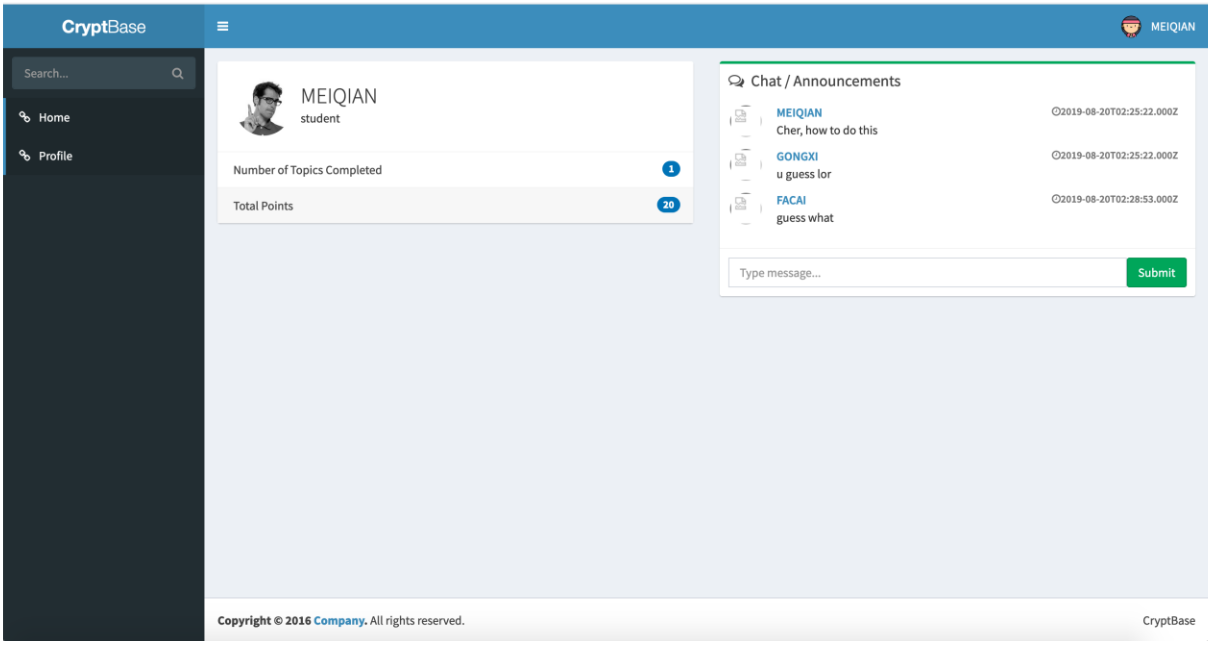
Question 2: Trapdoor Knapsack makes use of a difficult problem. What is it?

● A. Riemann Hypothesis
○ B.Subset Sum Problem
○ C.P vs. NP Problem.
○ D.Navier-Stokes Equation.

Congrats! You have completed the quiz!
Your score is 1

11.1.7. User Profile

Users can access their profile page, which enables them to view number of completed topic as well as their total learning points



MEIQIAN
student

Number of Topics Completed	1
Total Points	20

MEIQIAN 2019-08-20T02:25:22.000Z
Cher, how to do this

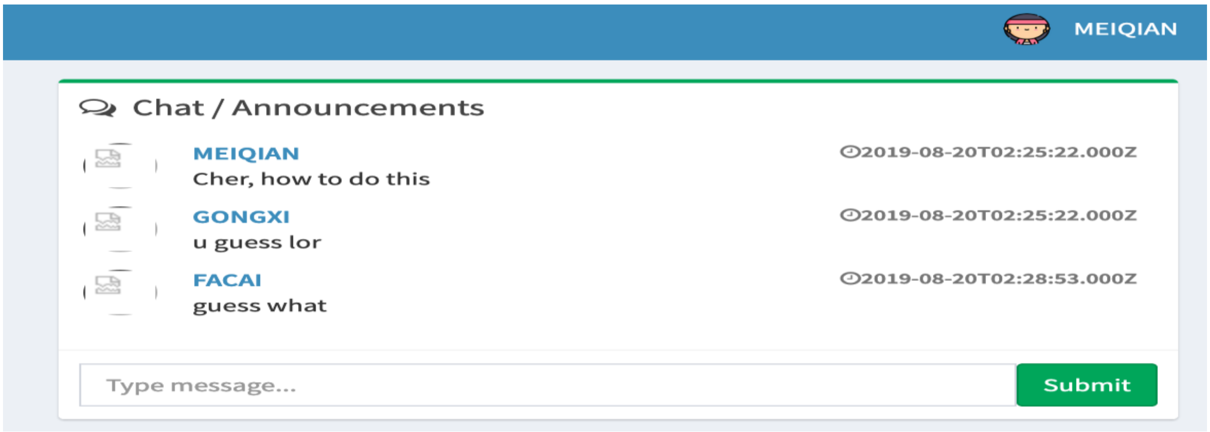
GONGXI 2019-08-20T02:25:22.000Z
u guess lor

FACAI 2019-08-20T02:28:53.000Z
guess what

Copyright © 2016 Company. All rights reserved.

11.1.8. Chat Function

Students and lecturers can communicate each other with the chat function in their user profile page. This is function enables the ease of communication between both parties as shown below:



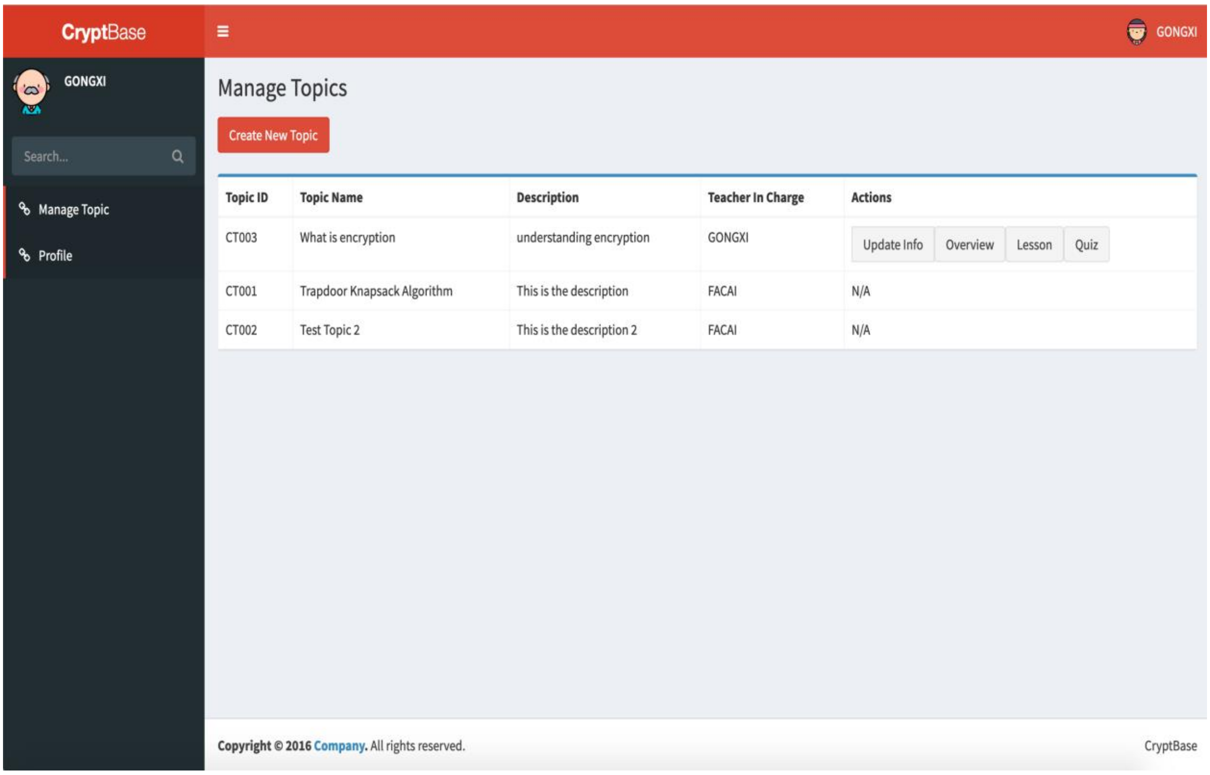
MEIQIAN
Cher, how to do this
2019-08-20T02:25:22.000Z

GONGXI
u guess lor
2019-08-20T02:25:22.000Z

FACAI
guess what
2019-08-20T02:28:53.000Z

11.1.9. Manage Topics as lecturer

Lecturers have access to manage topics such as creating, editing and deleting topics as shown below:

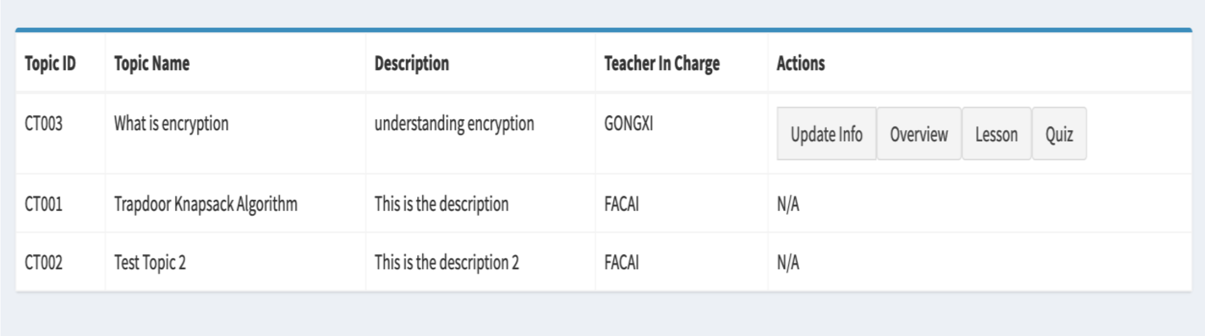


Topic ID	Topic Name	Description	Teacher In Charge	Actions
CT003	What is encryption	understanding encryption	GONGXI	Update Info Overview Lesson Quiz
CT001	Trapdoor Knapsack Algorithm	This is the description	FACAI	N/A
CT002	Test Topic 2	This is the description 2	FACAI	N/A

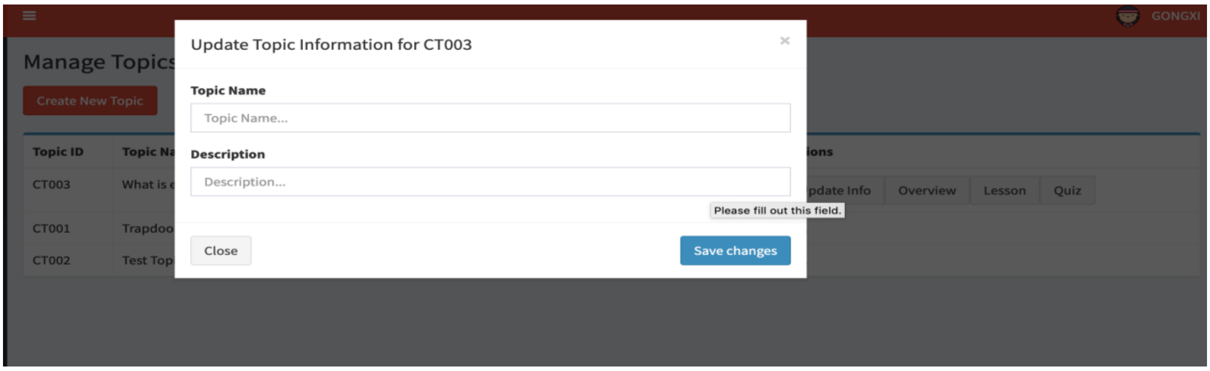
Copyright © 2016 Company. All rights reserved.

11.1.10. Topics Actions Features

Lecturer may update the content in the existing topic name, adding new lesson to topic, overview and adding quiz to the topic as shown below:



Topic ID	Topic Name	Description	Teacher In Charge	Actions
CT003	What is encryption	understanding encryption	GONGXI	Update Info Overview Lesson Quiz
CT001	Trapdoor Knapsack Algorithm	This is the description	FACAI	N/A
CT002	Test Topic 2	This is the description 2	FACAI	N/A



Update Topic Information for CT003

Topic Name

Topic Name...

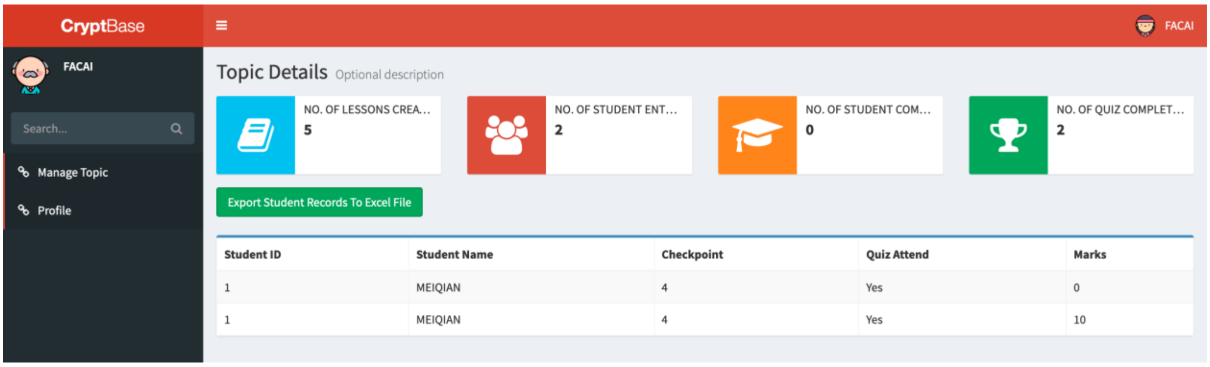
Description

Description...

Please fill out this field.

11.1.11. Topic Overview Function

The overview function allows the lecturer to the view the statistic of on how many students has been enrol to each topic, student learning progress and quiz attempt as well as their quiz result marks. Lecturers can export the students record of excel file to a local device as shown below:



Topic Details Optional description

NO. OF LESSONS CREA... 5

NO. OF STUDENT ENT... 2

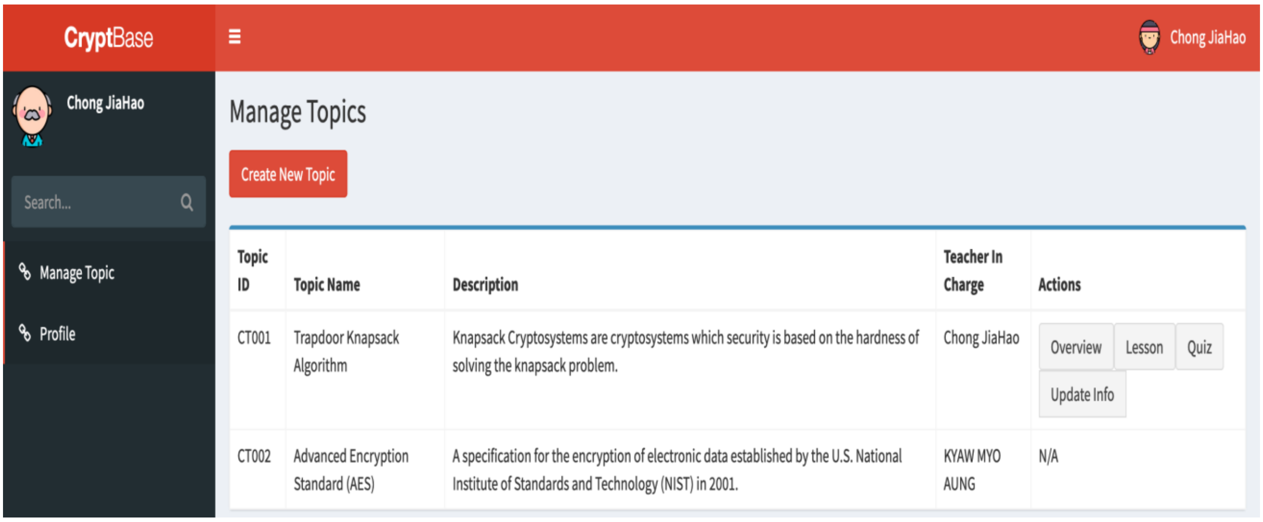
NO. OF STUDENT COM... 0

NO. OF QUIZ COMPLET... 2

Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1	MEIQIAN	4	Yes	0
1	MEIQIAN	4	Yes	10

11.1.12. Manage Lesson Function

Manage lesson function allows the lecturer to add additional lessons under a topic. Lecturer can use PowerPoint slide to upload as a lesson. Lecturer can also create lesson using HTML function. When a lesson is uploaded, lecturer will be able to view the pages live. The uploaded lessons can also be updated using "*Update*" button as shown below:

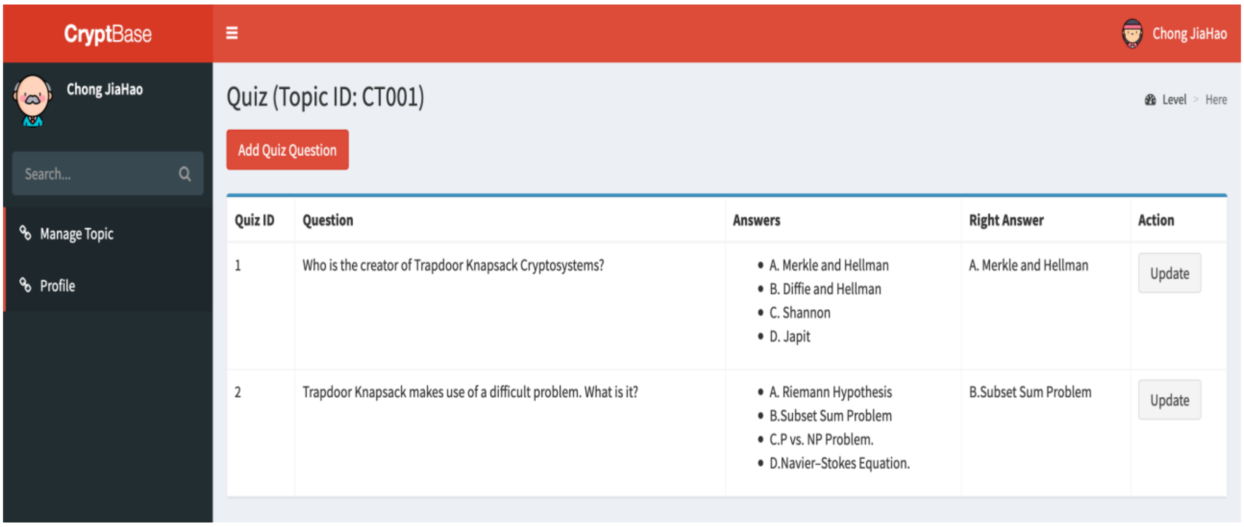


Manage Topics

Topic ID	Topic Name	Description	Teacher In Charge	Actions
CT001	Trapdoor Knapsack Algorithm	Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.	Chong JiaHao	Overview Lesson Quiz Update Info
CT002	Advanced Encryption Standard (AES)	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.	KYAW MYO AUNG	N/A

11.1.13. Manage Quiz Feature

Manage Quiz function for lecturer allow to set the multiple-choice questions for the students to try out for the knowledge test as shown below.

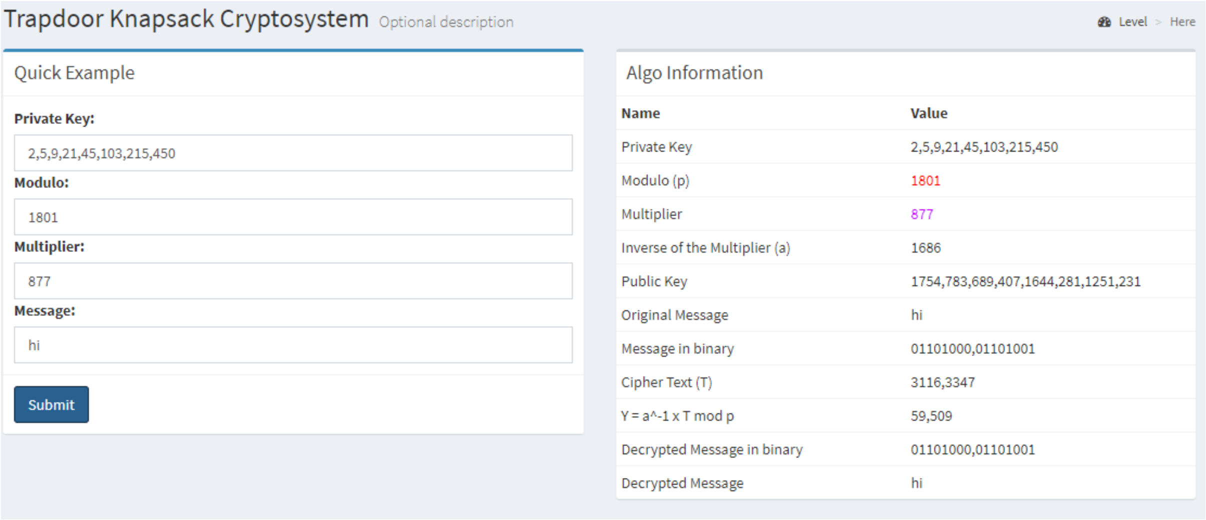


Quiz (Topic ID: CT001)

Quiz ID	Question	Answers	Right Answer	Action
1	Who is the creator of Trapdoor Knapsack Cryptosystems?	• A. Merkle and Hellman • B. Diffie and Hellman • C. Shannon • D. Japit	A. Merkle and Hellman	Update
2	Trapdoor Knapsack makes use of a difficult problem. What is it?	• A. Riemann Hypothesis • B.Subset Sum Problem • C.P vs. NP Problem. • D.Navier-Stokes Equation.	B.Subset Sum Problem	Update

11.1.14. Interactive Demo and Animated Explanation

The Trapdoor Knapsack calculation and animation page allows user to gain better understanding to the crypto system through interactive animation.



Trapdoor Knapsack Cryptosystem Optional description

Quick Example

Private Key: 2,5,9,21,45,103,215,450

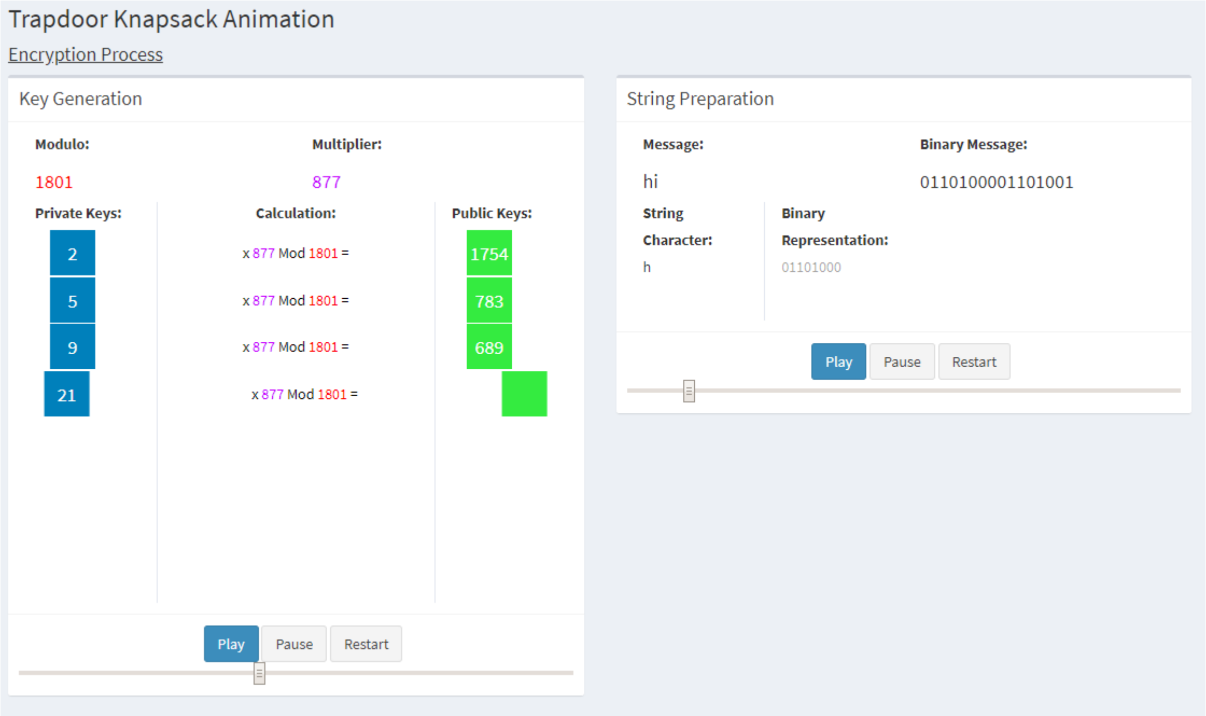
Modulo: 1801

Multiplier: 877

Message: hi

Algo Information

Name	Value
Private Key	2,5,9,21,45,103,215,450
Modulo (p)	1801
Multiplier	877
Inverse of the Multiplier (a)	1686
Public Key	1754,783,689,407,1644,281,1251,231
Original Message	hi
Message in binary	01101000,01101001
Cipher Text (T)	3116,3347
Y = a^-1 x T mod p	59,509
Decrypted Message in binary	01101000,01101001
Decrypted Message	hi



Trapdoor Knapsack Animation

Encryption Process

Key Generation

Modulo: 1801

Multiplier: 877

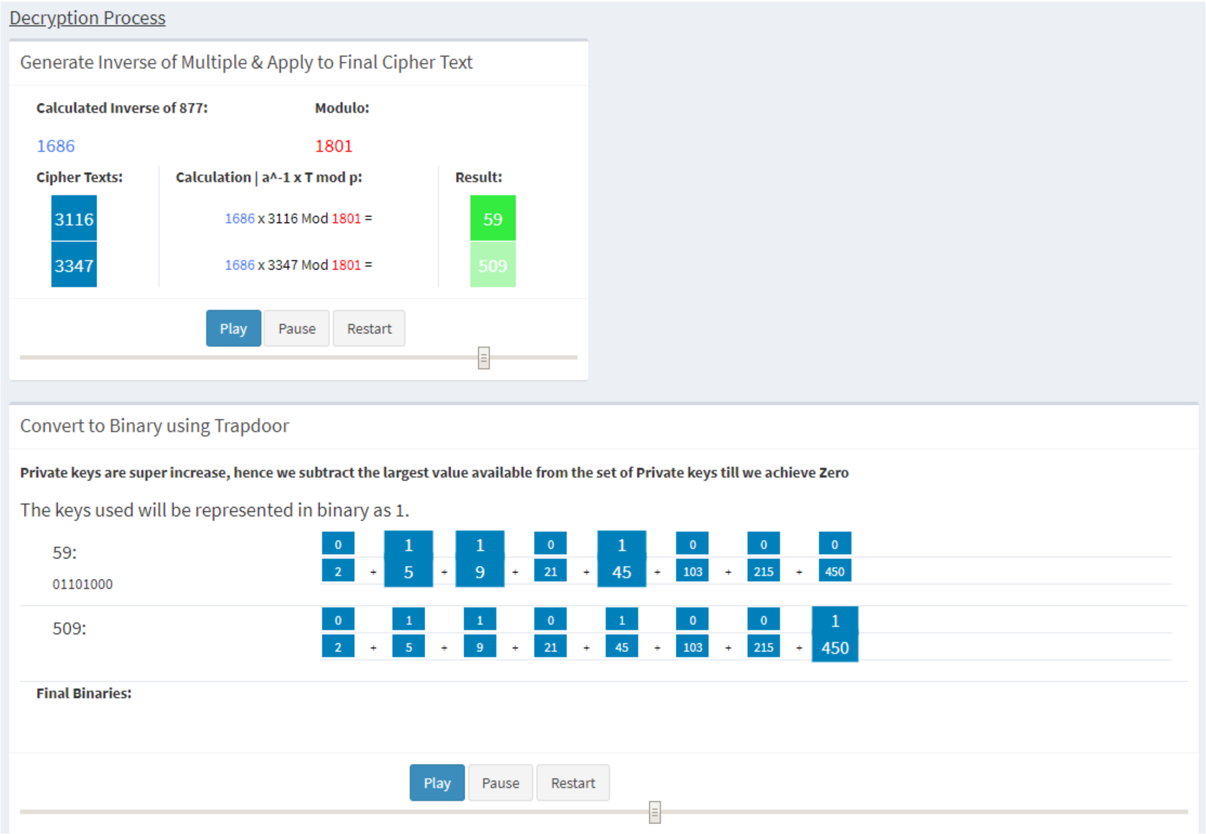
Private Keys:	Calculation:	Public Keys:
2	x 877 Mod 1801 =	1754
5	x 877 Mod 1801 =	783
9	x 877 Mod 1801 =	689
21	x 877 Mod 1801 =	

String Preparation

Message: hi

Binary Message: 0110100001101001

String Character:	Binary Representation:
h	01101000



Generate Inverse of Multiple & Apply to Final Cipher Text

Calculated Inverse of 877:	Modulo:
1686	1801

Cipher Texts:	Calculation | a^-1 x T mod p:	Result:
3116	1686 x 3116 Mod 1801 =	59
3347	1686 x 3347 Mod 1801 =	509

Convert to Binary using Trapdoor

Private keys are super increase, hence we subtract the largest value available from the set of Private keys till we achieve Zero

The keys used will be represented in binary as 1.

59: 01101000	0	1	1	0	1	0	0	0
	2 +	5 +	9 +	21 +	45 +	103 +	215 +	450
509:	0	1	1	0	1	0	0	1
	2 +	5 +	9 +	21 +	45 +	103 +	215 +	450

Final Binaries:

11.2. Non-Functional Features

Beside the function features, CryptBase also provide the following non-functional features such as:

- The system provides simple user interaction and user-friendly
- Users with internet connectivity will be able to access the system.
- There is no require installing the application on user's devices as CryptBase is the web application and can be used via Web Browser
- Since there is no installation require on the user devices, user can save their device storage
- User can access to CryptBase using either computer or their mobile phone
- The system is operating using open sources, so it is cost effective.
- CryptBase provide reliability and efficiency.

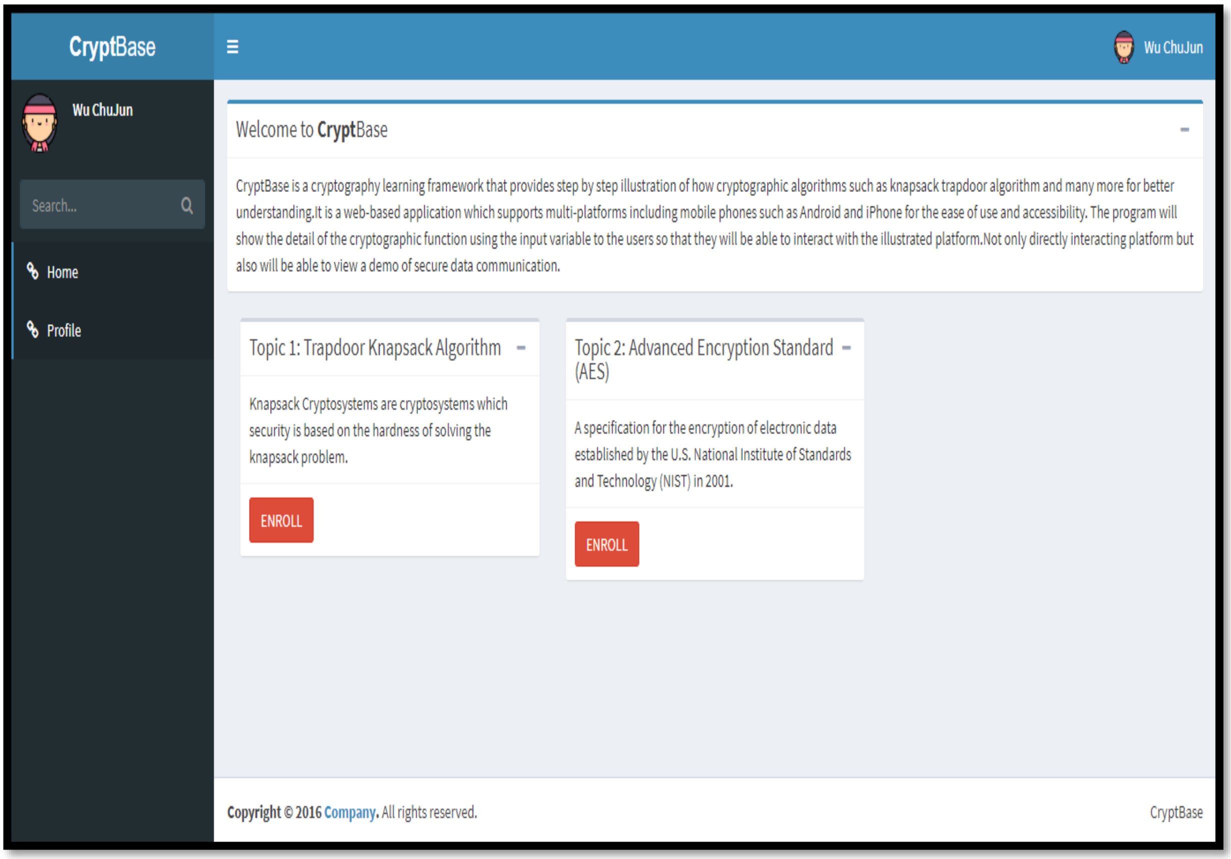
12. Test cases & UAT

12.1. Tasks as Student

12.1.1. Testing Login as Student

	Description of Task	Test Steps	Expected Result	Result	Remarks
	Login as Student	Login with credentials Username: 1001 Password: student1	Successful login would display homepage with blue coloured menu bar	PASS	

Screenshot:



Welcome to **Crypt**Base

CryptBase is a cryptography learning framework that provides step by step illustration of how cryptographic algorithms such as knapsack trapdoor algorithm and many more for better understanding.It is a web-based application which supports multi-platforms including mobile phones such as Android and iPhone for the ease of use and accessibility. The program will show the detail of the cryptographic function using the input variable to the users so that they will be able to interact with the illustrated platform.Not only directly interacting platform but also will be able to view a demo of secure data communication.

Topic 1: Trapdoor Knapsack Algorithm

Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.

Topic 2: Advanced Encryption Standard (AES)

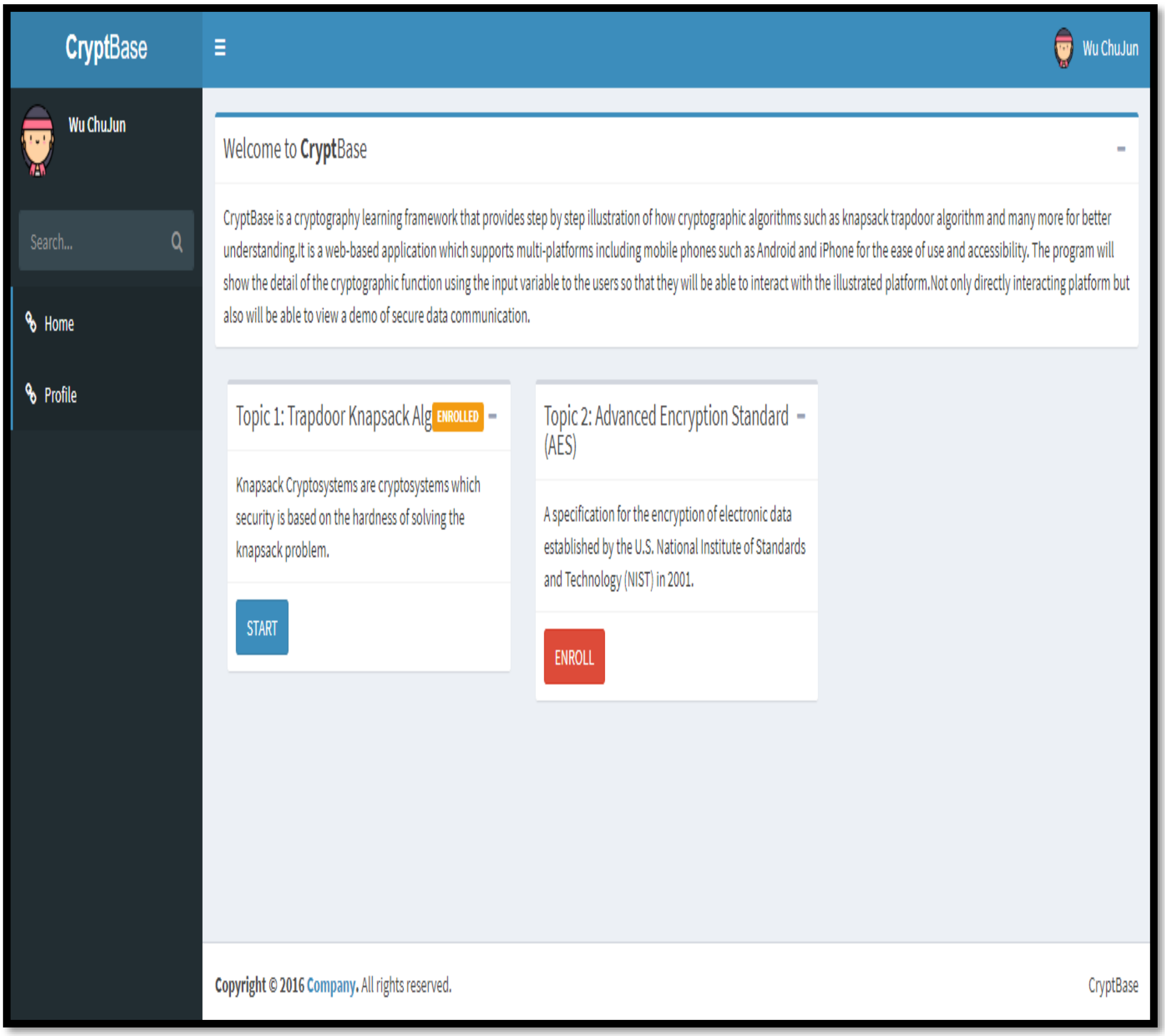
A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Copyright © 2016 Company. All rights reserved.

12.1.2. Testing Enrol into Topic

	Enrol into Topic	Click Enrol button	Upon successful enrolment, the button would change to “start”	PASS	

Screenshot:



Welcome to CryptBase

CryptBase is a cryptography learning framework that provides step by step illustration of how cryptographic algorithms such as knapsack trapdoor algorithm and many more for better understanding.It is a web-based application which supports multi-platforms including mobile phones such as Android and iPhone for the ease of use and accessibility. The program will show the detail of the cryptographic function using the input variable to the users so that they will be able to interact with the illustrated platform.Not only directly interacting platform but also will be able to view a demo of secure data communication.

Topic 1: Trapdoor Knapsack Alg ENROLLED

Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.

Topic 2: Advanced Encryption Standard (AES)

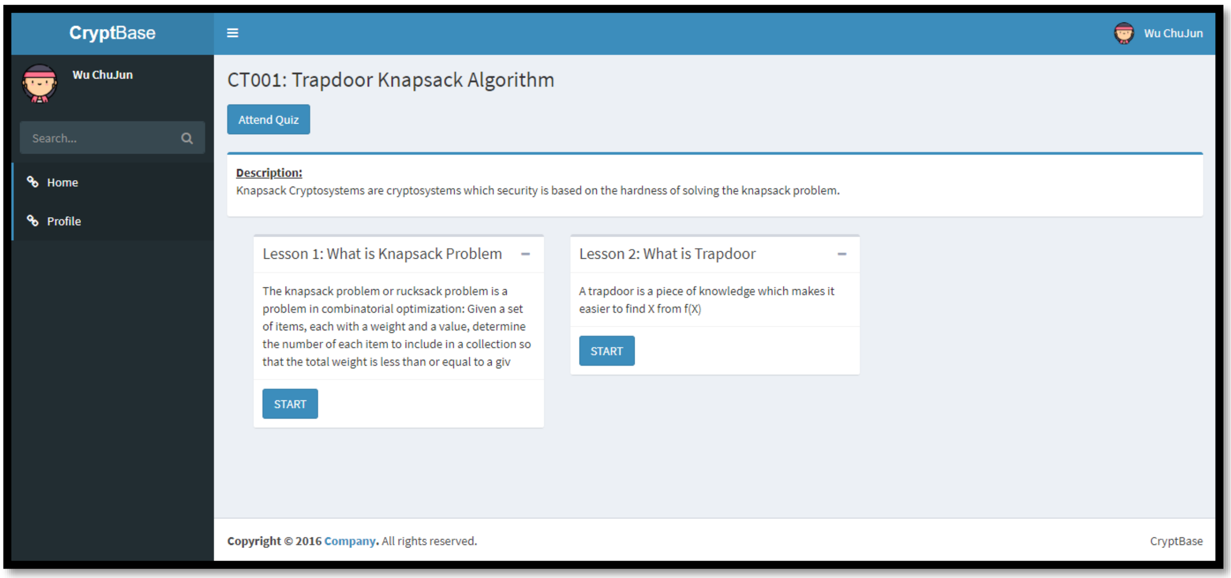
A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Copyright © 2016 Company. All rights reserved.

12.1.3. Start Topic Feature Test

	Start Topic	Click on Start Lesson button	Launch Lesson for the specific topic	PASS	

Screenshot:



CT001: Trapdoor Knapsack Algorithm

Description:
Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.

Lesson 1: What is Knapsack Problem

The knapsack problem or rucksack problem is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a giv

Lesson 2: What is Trapdoor

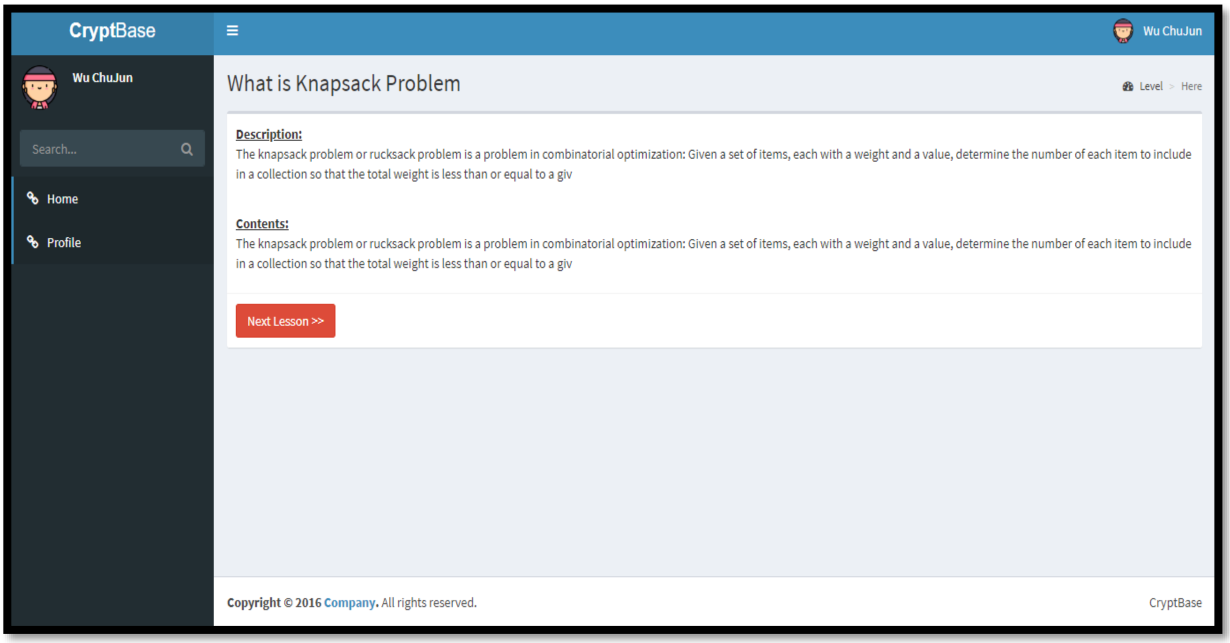
A trapdoor is a piece of knowledge which makes it easier to find X from f(X)

Copyright © 2016 Company. All rights reserved.

12.1.4. Testing on Attend Lesson 1

	Attend Lesson 1	Click start on Lesson 1	Display Lesson contents	PASS	

Screenshot:



What is Knapsack Problem

Description:
The knapsack problem or rucksack problem is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a giv

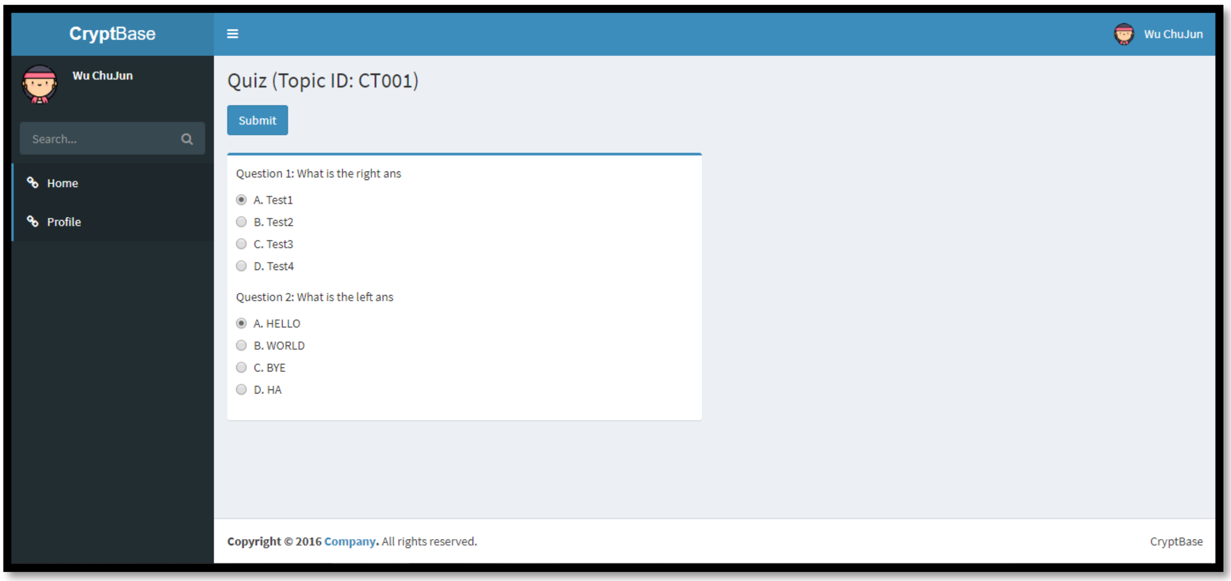
Contents:
The knapsack problem or rucksack problem is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a giv

Copyright © 2016 Company. All rights reserved.

12.1.5. Test Quiz Feature

	Attend Quiz	Click on attend quiz in individual topic page	Display Quiz for topic	PASS	

Screenshot:



Quiz (Topic ID: CT001)

Question 1: What is the right ans

● A. Test1
○ B. Test2
○ C. Test3
○ D. Test4

Question 2: What is the left ans

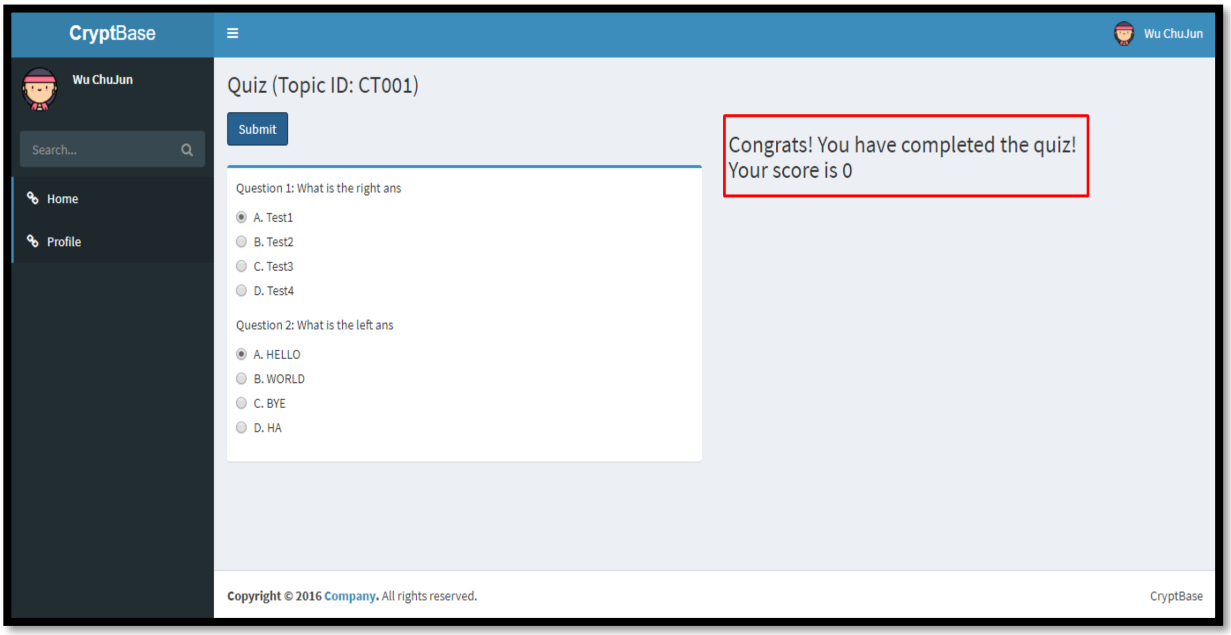
● A. HELLO
○ B. WORLD
○ C. BYE
○ D. HA

Copyright © 2016 Company. All rights reserved.

12.1.6. Quiz submission Test

	Submit Quiz	Click on Submit button	Display results for Quiz	PASS	

Screenshot:



Quiz (Topic ID: CT001)

Congrats! You have completed the quiz!
Your score is 0

Question 1: What is the right ans

● A. Test1
○ B. Test2
○ C. Test3
○ D. Test4

Question 2: What is the left ans

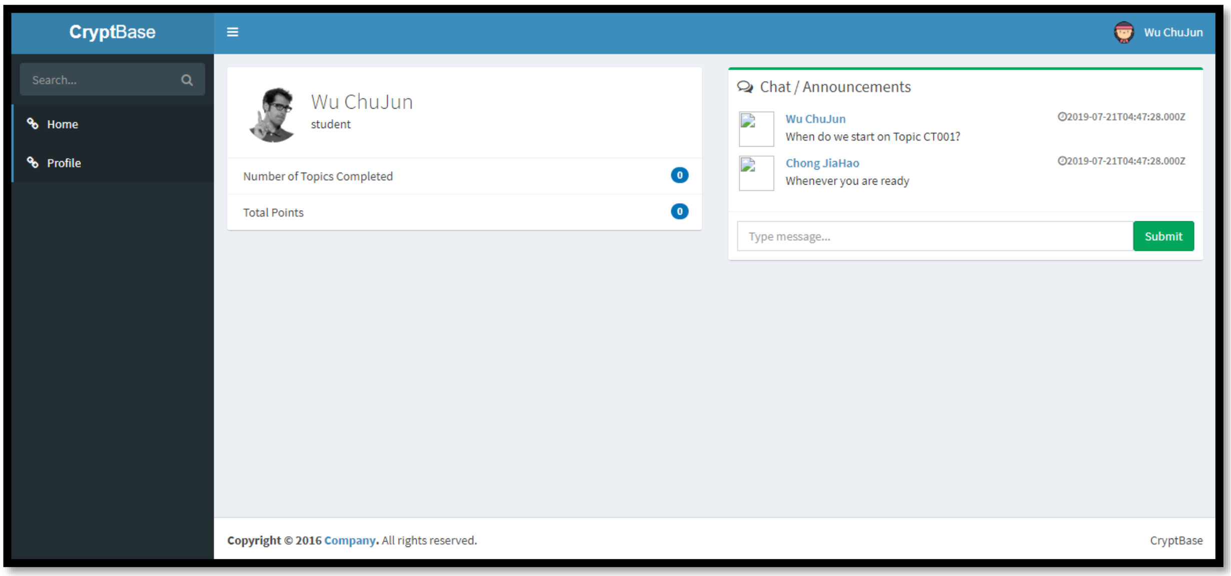
● A. HELLO
○ B. WORLD
○ C. BYE
○ D. HA

Copyright © 2016 Company. All rights reserved.

12.1.7. Profile Page Features

	Profile Page	Click on Profile Button	Display profile and Chat	PASS	

Screenshot:



Wu ChuJun
student

Number of Topics Completed 0

Total Points 0

Chat / Announcements

Wu ChuJun ⊙2019-07-21T04:47:28.000Z
When do we start on Topic CT001?

Chong JiaHao ⊙2019-07-21T04:47:28.000Z
Whenever you are ready

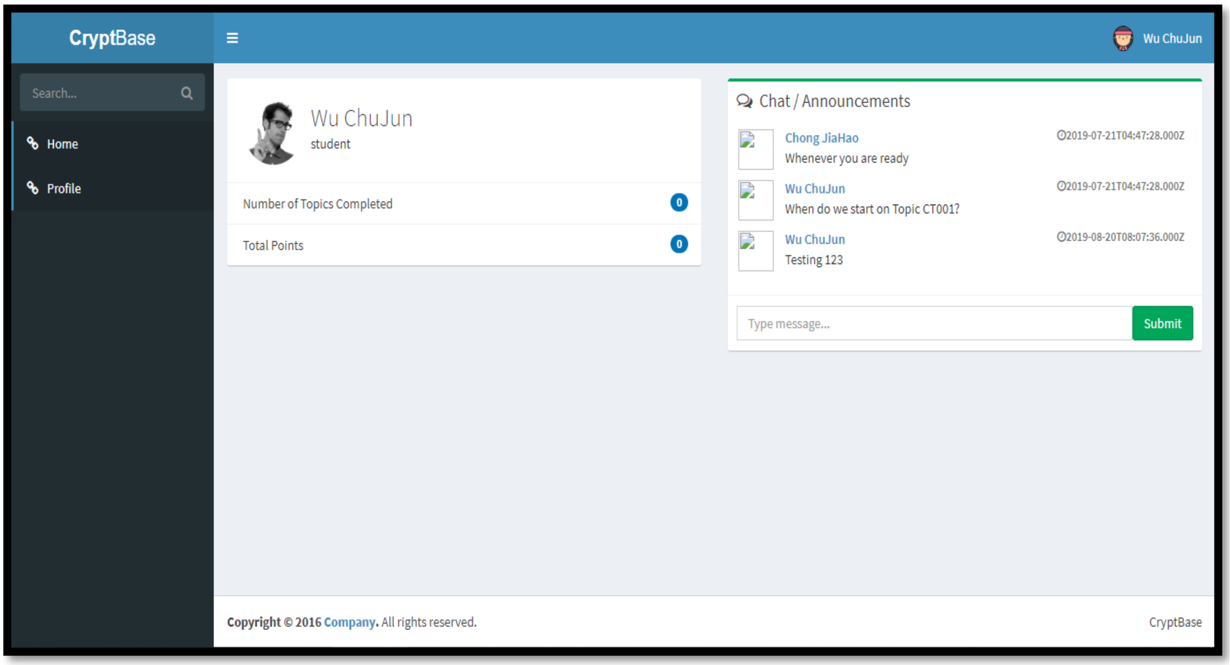
Type message...

Copyright © 2016 Company. All rights reserved.

12.1.8. Chat functional Test

	Update Chat	Write a sentence and update chat	Updated chat in chat box	PASS	

Screenshot:



Wu ChuJun
student

Number of Topics Completed 0

Total Points 0

Chat / Announcements

Chong JiaHao ⊙2019-07-21T04:47:28.000Z
Whenever you are ready

Wu ChuJun ⊙2019-07-21T04:47:28.000Z
When do we start on Topic CT001?

Wu ChuJun ⊙2019-08-20T08:07:36.000Z
Testing 123

Type message...

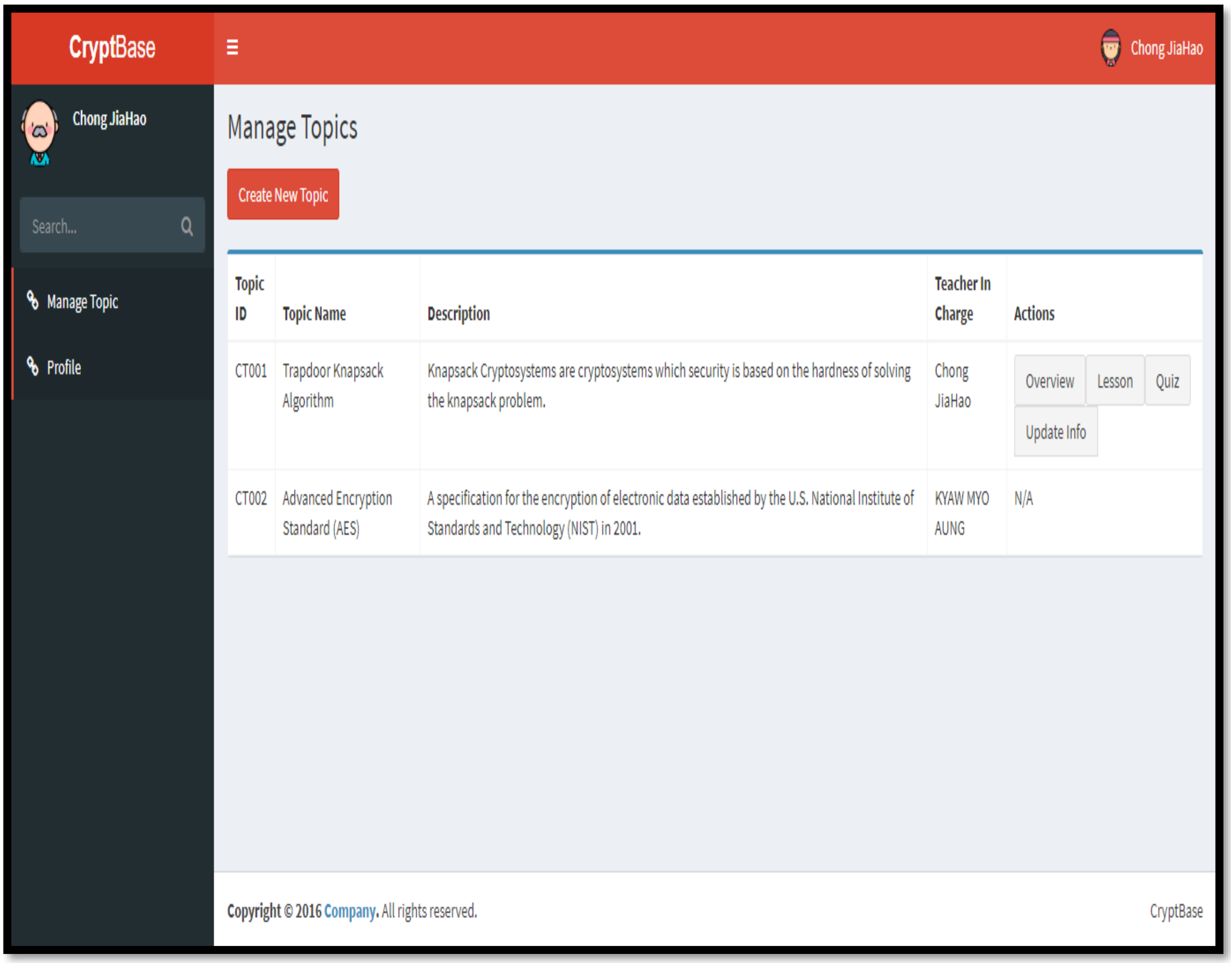
Copyright © 2016 Company. All rights reserved.

12.2. Tasks as Lecturer

12.2.1. Lecturer Login Test

	Description of Task	Test Steps	Expected Result	Result	Remarks
	Login as Lecturer	Login with credentials Username: 5001 Password: lecturer1	Successful login would display manage topic page with red coloured menu bar	PASS	

Screenshot:



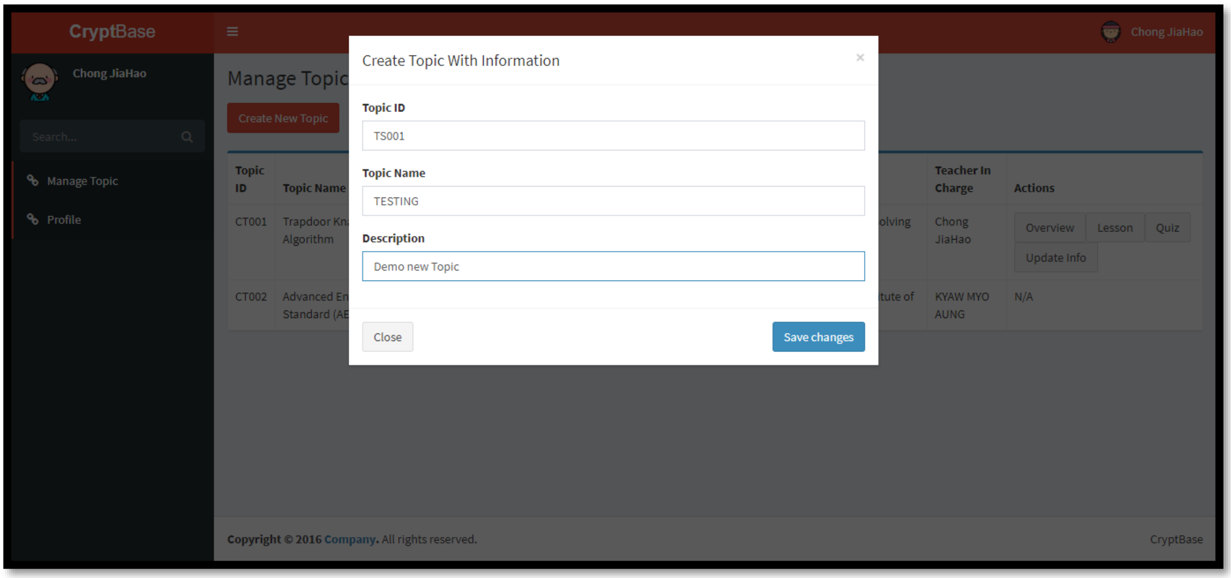
Topic ID	Topic Name	Description	Teacher In Charge	Actions
CT001	Trapdoor Knapsack Algorithm	Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.	Chong JiaHao	Overview Lesson Quiz Update Info
CT002	Advanced Encryption Standard (AES)	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.	KYAW MYO AUNG	N/A

Copyright © 2016 Company. All rights reserved. CryptBase

12.2.2. Topic Creation Feature Test

	Create new topic	Create new topic as Topicid: TS001 Topic Name: TESTING Description: Demo new topic	New topic to be displayed in Manage topic page	PASS	

Screenshot:



Create Topic With Information

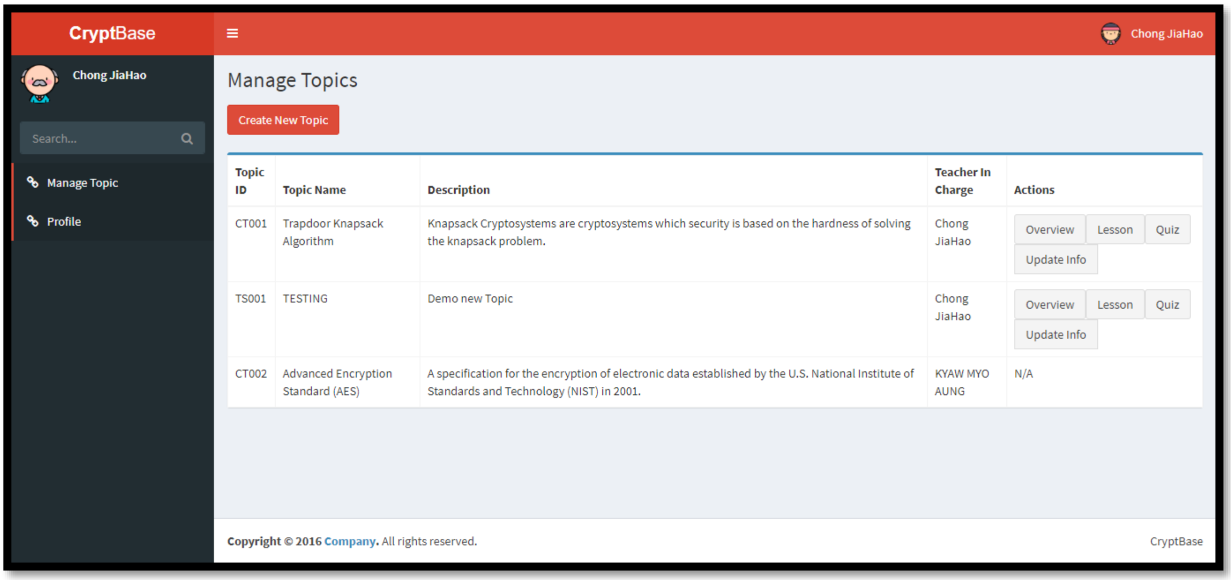
Topic ID: TS001

Topic Name: TESTING

Description: Demo new Topic

Close | Save changes

Copyright © 2016 Company. All rights reserved. CryptBase



Manage Topics

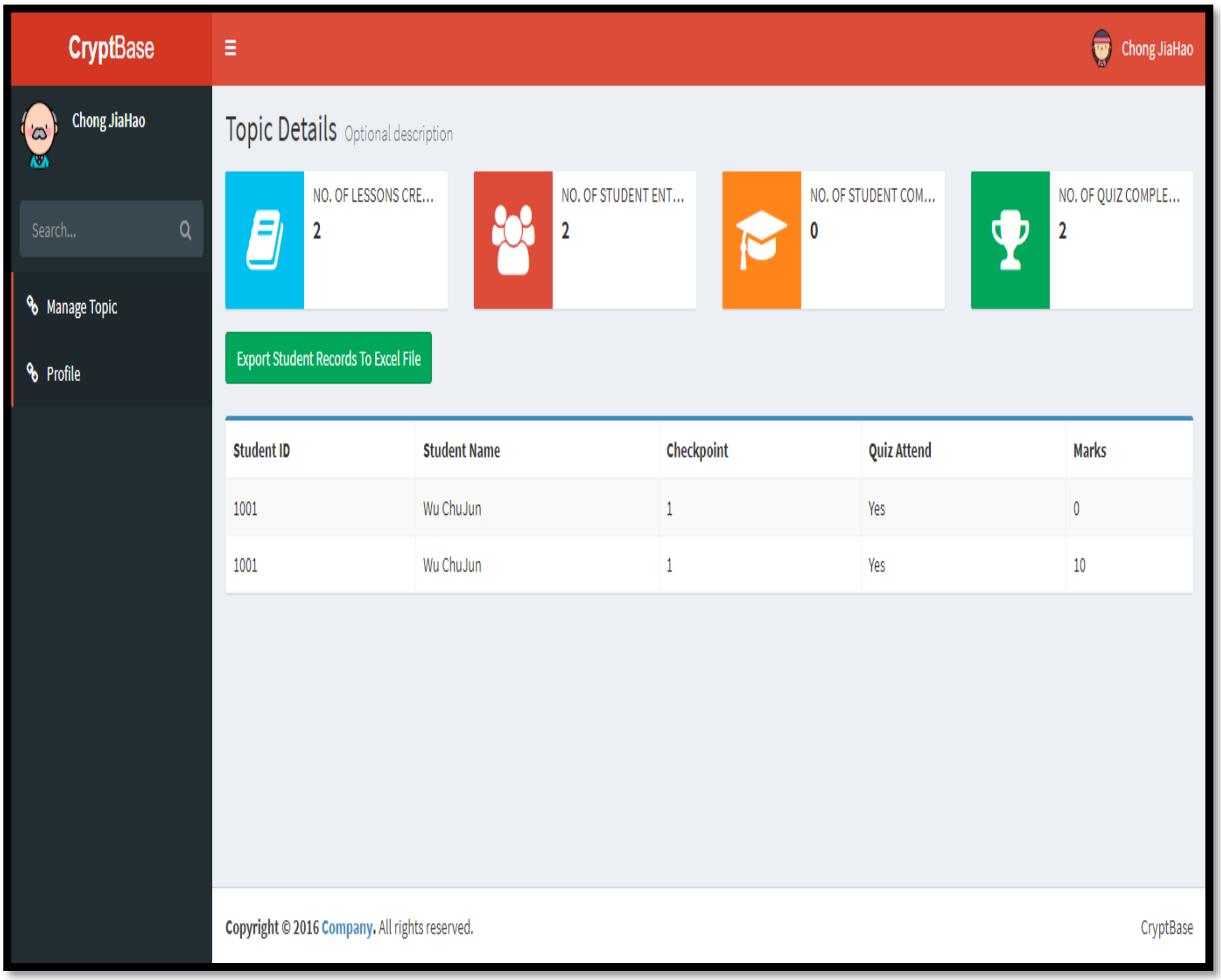
Topic ID	Topic Name	Description	Teacher In Charge	Actions
CT001	Trapdoor Knapsack Algorithm	Knapsack Cryptosystems are cryptosystems which security is based on the hardness of solving the knapsack problem.	Chong JiaHao	Overview Lesson Quiz Update Info
TS001	TESTING	Demo new Topic	Chong JiaHao	Overview Lesson Quiz Update Info
CT002	Advanced Encryption Standard (AES)	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.	KYAW MYO AUNG	N/A

Copyright © 2016 Company. All rights reserved. CryptBase

12.2.3. Test Topic Overview Feature

	Overview of a single topic	Click on overview for topic CT001	Display statistic of topic. Number of enrolled students, number of completed quiz, etc	PASS	

Screenshot:



CryptBase
Chong JiaHao
Chong JiaHao
Search...
Manage Topic
Profile
Export Student Records To Excel File
Copyright © 2016 Company. All rights reserved.
CryptBase

Topic Details Optional description

NO. OF LESSONS CRE... 2

NO. OF STUDENT ENT... 2

NO. OF STUDENT COM... 0

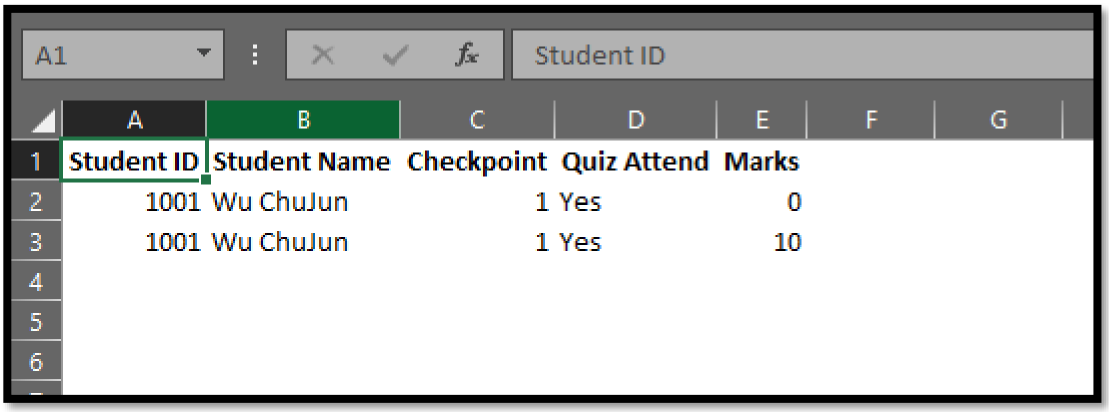
NO. OF QUIZ COMPLE... 2

Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1001	Wu ChuJun	1	Yes	0
1001	Wu ChuJun	1	Yes	10

12.2.4. Topic Statistic Export Feature Test

	Export topic statistic	Export excel	Display statistic of topic in excel	PASS	

Screenshot:

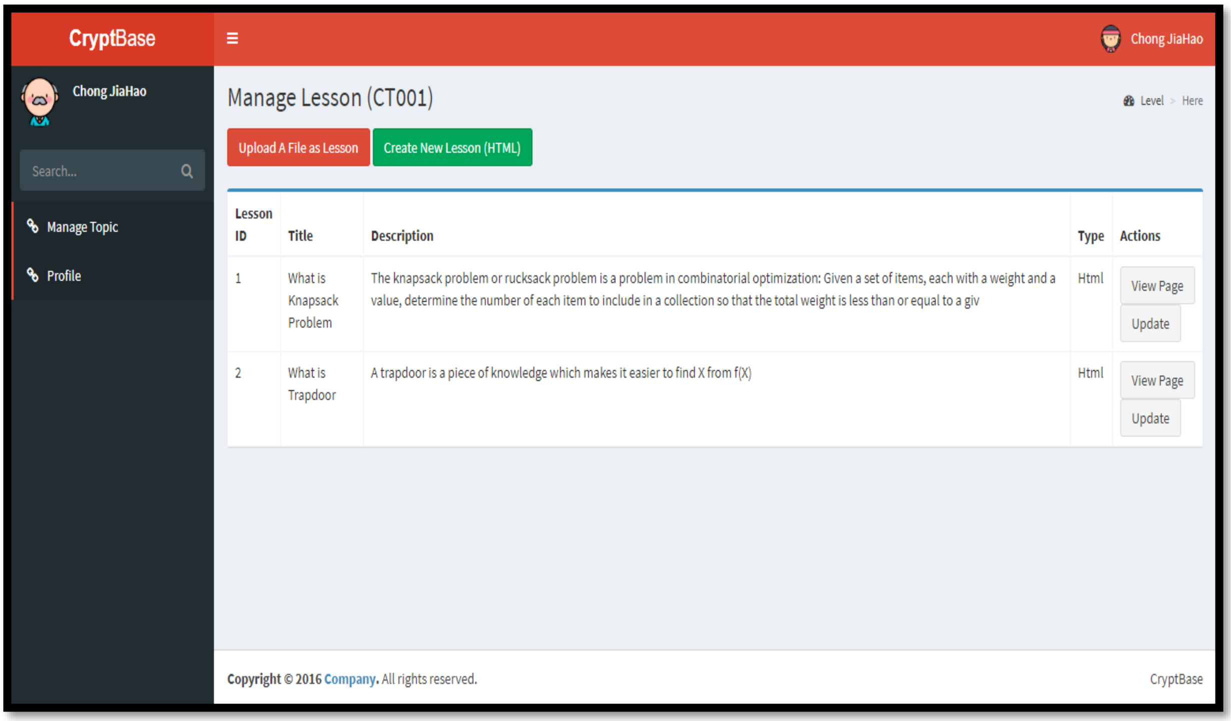


Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1001	Wu ChuJun	1	Yes	0
1001	Wu ChuJun	1	Yes	10

12.2.5. Manage Lesson Feature Test

	Manage Lesson	Click on Manage lesson to edit lesson details	Display manage lesson page	PASS	

Screenshot:



Manage Lesson (CT001)

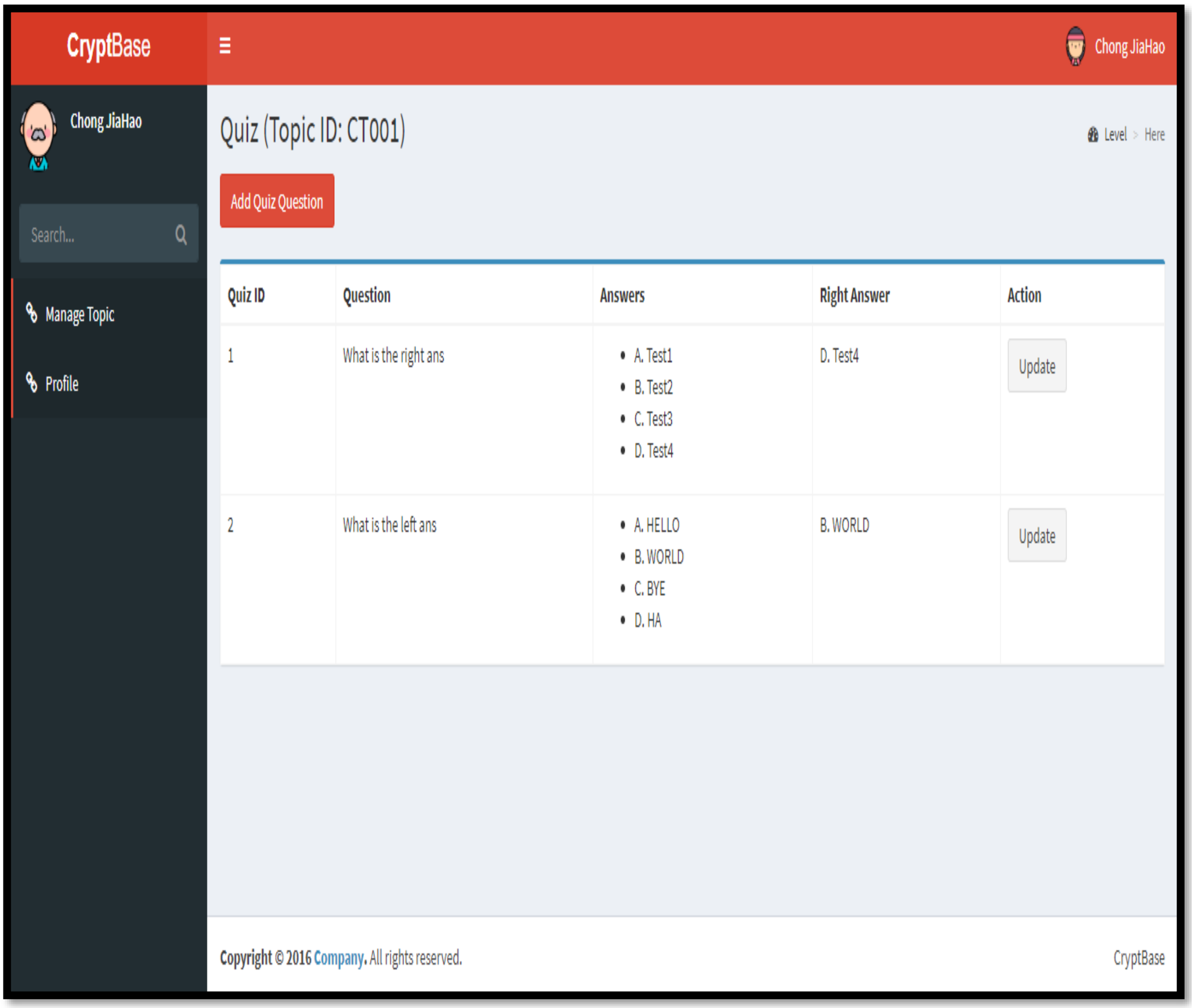
Lesson ID	Title	Description	Type	Actions
1	What is Knapsack Problem	The knapsack problem or rucksack problem is a problem in combinatorial optimization: Given a set of items, each with a weight and a value, determine the number of each item to include in a collection so that the total weight is less than or equal to a giv	Html	View Page Update
2	What is Trapdoor	A trapdoor is a piece of knowledge which makes it easier to find X from f(X)	Html	View Page Update

Copyright © 2016 Company. All rights reserved. CryptBase

12.2.6. Manage Quiz Feature Test

	Manage Quiz	Click on manage quiz to edit quiz questions	Display manage quiz page	PASS	

Screenshot:



Quiz (Topic ID: CT001)

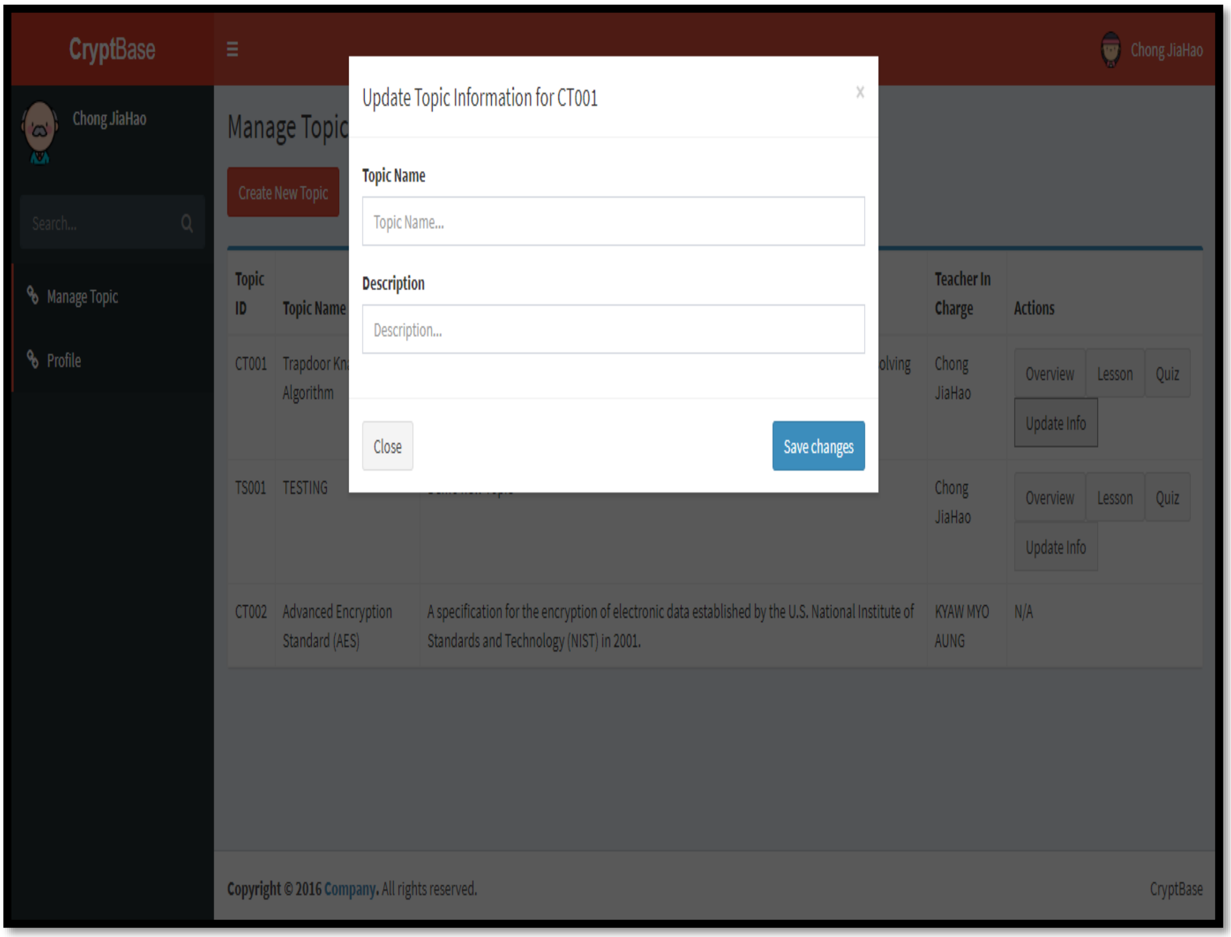
Quiz ID	Question	Answers	Right Answer	Action
1	What is the right ans	• A. Test1 • B. Test2 • C. Test3 • D. Test4	D. Test4	Update
2	What is the left ans	• A. HELLO • B. WORLD • C. BYE • D. HA	B. WORLD	Update

Copyright © 2016 Company. All rights reserved.

12.2.7. Update Topic Feature Test

	Update Topic Details	Click on update info	Pop-out window for topic update	PASS	

Screenshot:



Update Topic Information for CT001

Topic Name

Topic Name...

Description

Description...

Topic ID	Topic Name		Teacher In Charge	Actions
CT001	Trapdoor Kn Algorithm	olving	Chong JiaHao	Overview Lesson Quiz Update Info
TS001	TESTING		Chong JiaHao	Overview Lesson Quiz Update Info
CT002	Advanced Encryption Standard (AES)	A specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.	KYAW MYO AUNG	N/A

Copyright © 2016 Company. All rights reserved.

13. Meeting Minutes

13.1. Meeting #1

Meeting:	Project Phase 1 – Meeting #1		
Date of Meeting: (DD-MMM-YYYY)	16 April 2019	***Time:***	18:45 Hrs
Location:	@ SIM HQ, Blk A2.09C		

1. Meeting Agenda

- Project Overview
- Timeline
- Task Allocation
- Discussion on Architecure Design

2. Attendees

Name	**Student Number**	**E-mail**
Dr. Loo Poh Kok	Supervisor	lubg9@outlook.com
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Introduction of Supervisor and Team members.
- Align expectations of project title
- To assign team roles & Responsibilities

4. To Do list

- Discussion on project proposal

13.2. Meeting #2

Meeting:	Project Phase 1 – Meeting #2		
Date of Meeting: (DD-MMM-YYYY)	20 April 2019	Time:	12:00 Hrs
Location:	@ SIM HQ, Blk B2.17		

1. Meeting Agenda

- Project Proposal Comfimation
- Design dussion

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Confirmation of Proposal documents

4. To Do list

- UI Designing
- Database platform
- Trapdoor algorithm

13.3. Meeting #3

Meeting:	Project Phase 1 – Meeting #3		
Date of Meeting: (DD-MMM-YYYY)	2 May 2019	Time:	18:30 Hrs
Location:	@ SIM HQ, Blk A 5.14		

1. Meeting Agenda

- Review on Proposal Draft Documet

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Market analysis
- Product features

4. To Do list

- Business value
- Web Template research

13.4. Meeting #4

Meeting:	Project Phase 1 – Meeting #4		
Date of Meeting: (DD-MMM-YYYY)	7 May 2019	Time:	18:30 Hrs
Location:	@ SIM HQ, Blk B 5.15		

1. Meeting Agenda

- Finalized Proposal Document

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- UI Confirmation (Backend page AdminLTE)
- Trapdoor algorithm

4. To Do list

- Database planning
- Presentation of lesson

13.5. Meeting #5

Meeting:	Project Phase 1 – Meeting #5		
Date of Meeting: (DD-MMM-YYYY)	16 May 2019	Time:	18:30 Hrs
Location:	@ SIM HQ, Blk B 5.15		

1. Meeting Agenda

- Web Content discussion

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Presentation of Lessons

4. To Do list

- Lesson Topics for Trapdoor
- Coding method & compilation

13.6. Meeting #6

Meeting:	Project Phase 1 – Meeting #6		
Date of Meeting: (DD-MMM-YYYY)	6 Jul 2019	Time:	10:00AM
Location:	Blk B @ SIM HQ		

1. Meeting Agenda

- Phase1 Prototype preparation

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Project Presentation discussion about Phase 1 Demo
- Details discussion about Database Design

4. To Do list

- Preliminary Tech Docs
- Preliminary User Guide

13.7. Meeting #7

Meeting:	Project Phase 2 – Meeting #1		
Date of Meeting: (DD-MMM-YYYY)	13 Jul 2019	Time:	2:30PM
Location:	Blk B @ SIM HQ		

1. Meeting Agenda

- Implementation update discussion

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Phase 1 Demo discussion with project supervisor before Project Presentation
- Discussion on function features

4. To Do list

- Prepare Project timeline docs update
- Coding approach on function feature implementations

13.8. Meeting #8

Meeting:	Project Phase 2 – Meeting #2		
Date of Meeting: (DD-MMM-YYYY)	27 Jul 2019	Time:	10:30AM
Location:	Blk B 5.15 @ SIM HQ		

1. Meeting Agenda

- Implementation update discussion

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Progress on current implementation status
- Discussion on issues items and debugging

4. To Do list

- Continues on the functional features
- Implementations on database information

13.9. Meeting #9

Meeting:	Project Phase 2 – Meeting #3		
Date of Meeting: (DD-MMM-YYYY)	4 Aug 2019	Time:	10:30AM
Location:	Blk B 5.15 @ SIM HQ		

1. Meeting Agenda

- Finalizing the implementation

2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item

- Progress on animation blocks & detail discussion
- Discussion on lecturer functions such as upload/downloading files
- Discussion on login page linking to database users

4. To Do list

- Finalize on animated feature
- To Finalize lecturer features & focus on quiz function
- Implementation on user profile & forum chat features

13.10. Meeting #10

Meeting:	Project Phase 2 – Meeting #4		
Date of Meeting: (DD-MMM-YYYY)	16 Aug 2019	Time:	10:30AM
Location:	Blk B 5.15 @ SIM HQ		

1. Meeting Agenda
• Discussion on Project documentation
2. Attendees

Name	Student Number	E-mail
CHONG JIAHAO	4799276	jhchong009@mymail.sim.edu.sg
MARCUS TAN YONGHUA	6212621	ymtan018@mymail.sim.edu.sg
WU CHUJUN	5988329	cwu014@mymail.sim.edu.sg
Kyaw Myo Aung , Johns	6097868	Myoak001@mymail.sim.edu.sg

3. Discussed Item
• Product testing • Discussion of project documentation
4. To Do list
• Coding finalization and hotfixes • Project video and Tech /user guide documentation

14. Appendix

14.1. Appendix A – Project Timeline

Project Timeline v1.1.xlsx

14.2. Appendix B – Demo Youtube Video

Part	URL
SSP19 2C Demo1 Deployment	https://youtu.be/dTwrynizY0A
SSP19 2C Demo2 Functions UserGuide	https://youtu.be/ghVSoakWxVo
SSP19 2C Demo3 Trapdoor Knapsack Simulator	https://youtu.be/LER8TPbZP00

14.3. Appendix C – Github

https://github.com/Surfaze/CryptBase

14.4. Appendix D – Hosting

CryptBase will be hosted on http://118.201.197.221:7000 for a limited time.

15. Reference

Rational Unified Process

https://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251_bestpractices_TP026B.pdf

Using RUP/UP

http://hosteddocs.ittoolbox.com/RP092305.pdf

Knapsack Algorithm step by step explanation

https://www.dotnetforall.com/knapsack-algorithm-with-easy-code-explanation-and-example/

Knapsack encryption &amp; decryption

http://mercury.webster.edu/aleshunas/COSC%205130/J-Knapsack.pdf

Knapsack encryption and simulation

https://asecuritysite.com/encryption/knap

Knapsack-type Cryptographic system

https://pdfs.semanticscholar.org/8586/ebdf8cfc338a45d8e853d2100b33b0e724b2.pdf

MySQL

https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html

What is NodeJS

https://en.wikipedia.org/wiki/Node.js

BootStrap Front-end Framework

https://en.wikipedia.org/wiki/Bootstrap_(front-end_framework)

Introduction to GitHub

https://www.howtogeek.com/180167/htg-explains-what-is-github-and-what-do-geeks-use-it-for/

What is Ubuntu

https://en.wikipedia.org/wiki/Ubuntu

NetBeans IDE

https://en.wikipedia.org/wiki/NetBeans