

UNIVERSITY OF WOLLONGONG



Bachelor of Computer Science - Digital Systems Security

CryptBase

Trapdoor Knapsack Simulator

User Manual

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/>>

User Manual Content

General	3
Installation	3
Access CryptBase Web Application	3
Chat	4
Student	6
Enroll a Topic	6
Start / Continue a Topic	6
Start a Lesson	7
How To Use Trapdoor Knapsacks Simulator	9
Attend a Quiz	11
View Profile	13
Lecturer	14
Manage Topics	14
Topic Overview	14
Export Student Records	15
Create New Topic	16
Update Topic Information	18
Manage Lessons	19
Create a HTML Lesson	19
Upload a file as lesson	22
Manage Quiz	24
Add quiz question	24
Change a quiz question	25

General

Installation

Refer to step by step installation attached below.

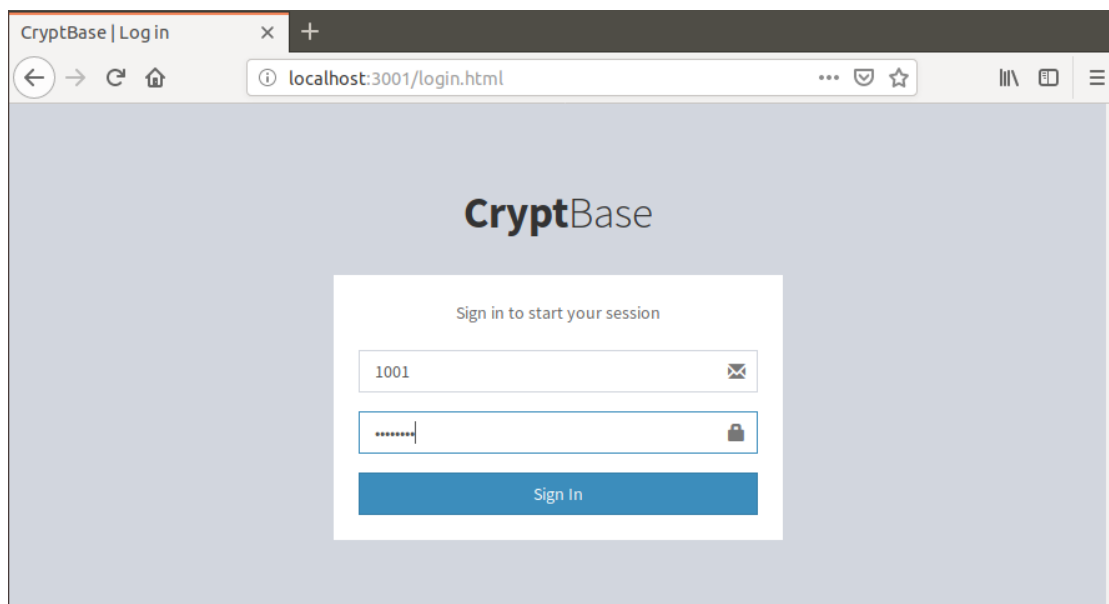


Final Deployment
Guide.pdf

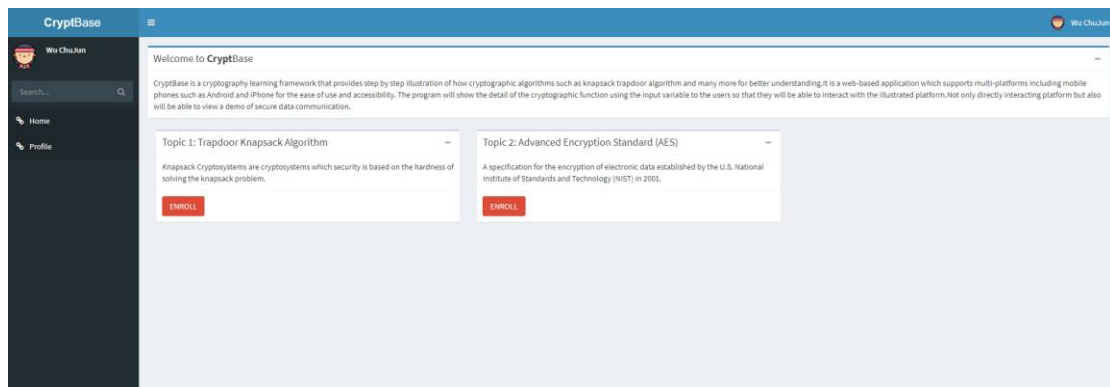
Access CryptBase Web Application

1. Open a browser, access URL: `http://serverIPAddress:3001`.
(E.g. `http://localhost:3001`)
2. Enter user id and password (credentials below)

Username	:	Password
1001		student1
1002		studetn2
5001		lecturer
5002		lecturer



3. Login successfully.

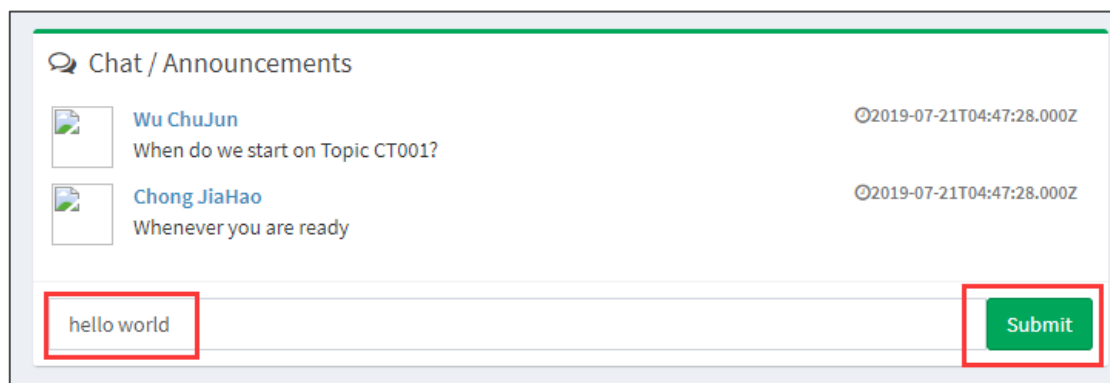


Chat

1. Go to Profile Page (<http://serverIPaddress:3001/profile>)




2. Type in your message and submit



3. Done.


Chat / Announcements



Wu ChuJun

When do we start on Topic CT001?


2019-07-21T04:47:28.000Z



Chong JiaHao

Whenever you are ready

2019-07-21T04:47:28.000Z



Wu ChuJun

hello world

2019-08-21T05:44:34.000Z

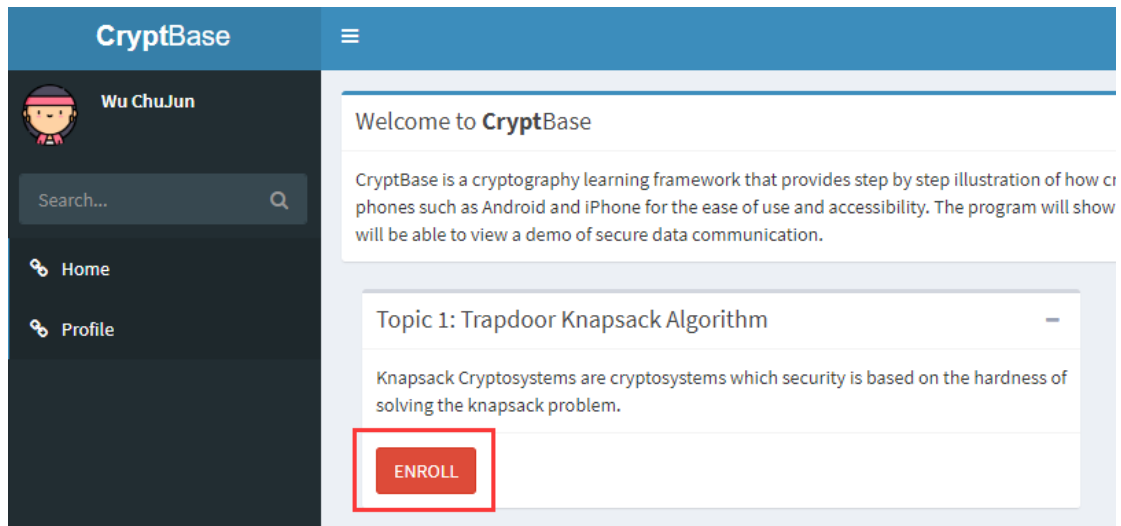
Type message...

Submit

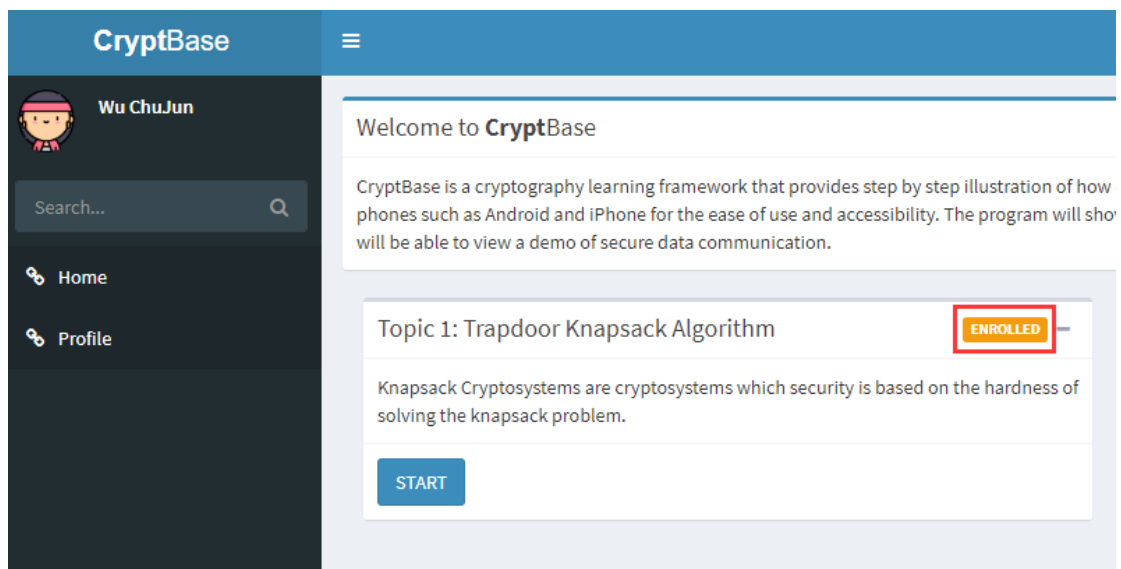
Student

Enroll a Topic

1. At the home page: <http://serverIPAddress:3001/home>, use “CryptBase” Logo or “Home” button to go back to the home page.
2. Click on the “ENROLL” button to enroll in the topic.



3. Successfully enrolled.



Start / Continue a Topic

1. At the home page: <http://serverIPAddress:3001/home>, use “CryptBase” Logo or “Home” button to go back to the home page.

2. Click on the “START” button to enter the topic lesson page after enrolled in the topic successfully.

The screenshot shows the CryptBase dashboard. On the left is a dark sidebar with the user's name 'Wu ChuJun', a search bar, and links for 'Home' and 'Profile'. The main content area has a blue header with the 'CryptBase' logo and a hamburger menu. Below the header, a welcome message is followed by a description of the platform. The 'Topic 1: Trapdoor Knapsack Algorithm' section is highlighted with an orange 'ENROLLED' tag. A blue 'START' button is visible at the bottom of this section, enclosed in a red rectangular box.

Start a Lesson

1. At the topic page (<http://serverIPaddress:3001/attendTopic/TopicID>)

The screenshot shows the 'CT001: Trapdoor Knapsack Algorithm' topic page. The sidebar is identical to the dashboard. The main content area has a blue header with the topic title and an 'Attend Quiz' button. Below this, a 'Description' section explains the knapsack problem. Two lesson cards are displayed: 'Lesson 1: What is Knapsack Problem' and 'Lesson 2: What is Trapdoor'. The 'Lesson 1' card contains a detailed description of the knapsack problem and has a blue 'START' button at the bottom, which is highlighted with a red rectangular box. The 'Lesson 2' card contains a brief definition of a trapdoor and also has a 'START' button.

2. Click on the “START” button to access the lesson.

The screenshot shows the CryptBase web application. The top header is blue with the 'CryptBase' logo on the left and a user profile 'Wu ChuJun' on the right. A dark sidebar on the left contains a search bar and links for 'Home' and 'Profile'. The main content area has a title 'What is Knapsack Problem' and a breadcrumb 'Level > Here'. Below the title, there is a 'Description' section explaining the knapsack problem, followed by a 'Contents' section detailing its history and applications. At the bottom of the content area, there is a red button labeled 'Next Lesson >>'.

3. Use “Next Lesson >>” Or “<< Previous Lesson” to access previous or next lesson

This screenshot shows the 'What is Trapdoor' lesson page in the CryptBase application. The layout is consistent with the previous screenshot, featuring the same header, sidebar, and main content area. The main content area includes a 'Description' of a trapdoor and a 'Contents' section. At the bottom of the content area, two buttons are highlighted with a red rectangle: '<< Previous Lesson' and 'Next Lesson >>'.

How To Use Trapdoor Knapsacks Simulator

1. To start animation, user to key in information in input fields. Note: separate multiple Private Keys with comma (,).

Trapdoor Knapsack Cryptosystem Optional description

👤 Level > Here

Quick Example

Private Key:

2,5,9,21,45,103,215,450

Modulo:

1801

Multiplier:

877

Message:

hi

Submit

Algo Information

Name	Value
Private Key	
Modulo (p)	
Multiplier	
Inverse of the Multiplier (a)	
Public Key	
Original Message	
Message in binary	
Cipher Text (T)	
$Y = a^{-1} \times T \bmod p$	
Decrypted Message in binary	
Decrypted Message	

Trapdoor Knapsack Animation

Encryption Process

Key Generation

Play

Pause

Restart

String Preparation

Play

Pause

Restart

2. Press Submit to generate Information regarding the encryption and decryption process. Animations will also be generated.

Trapdoor Knapsack Cryptosystem

Optional description

Level > Here

Quick Example

Private Key:

2,5,9,21,45,103,215,450

Modulo:

1801

Multiplier:

877

Message:

hi

Submit

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
$Y = a^{-1} \times T \bmod p$	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:

String Preparation

Message:

hi

Binary Message:

0110100001101001

String

Binary

Trapdoor Knapsack Animation

[Encryption Process](#)

Key Generation

Modulo:

1801

Multiplier:

877

Private Keys:

Calculation:

Public Keys:

Play

Pause

Restart

String Preparation

Message:

hi

Binary Message:

0110100001101001

String

Binary

Character:

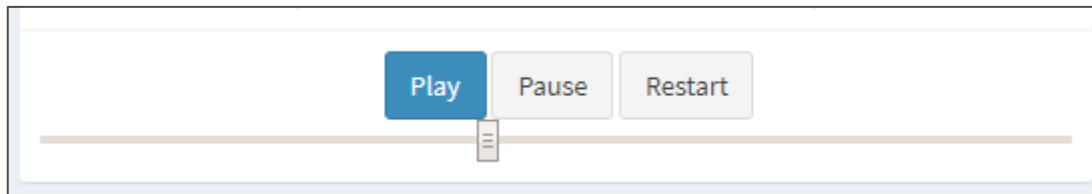
Representation:

Play

Pause

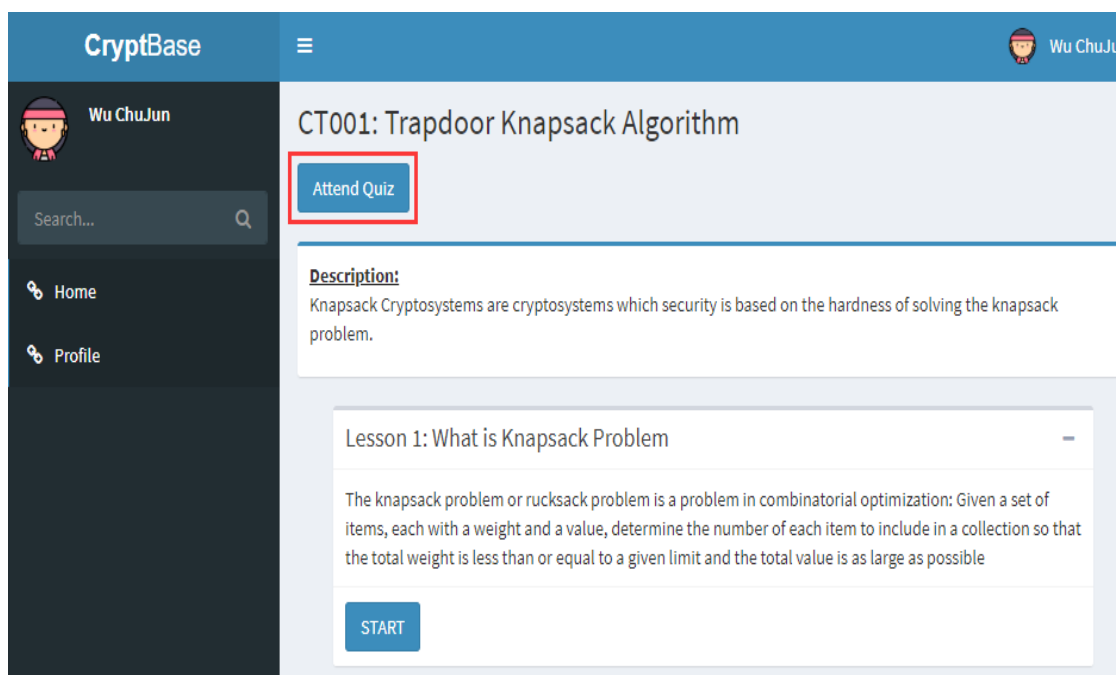
Restart

3. Users are able to make use of the Timeline Controls to navigate through the animation process.
 - a. Play to start the animation
 - b. Pause to pause the animation
 - c. Restart to restart the animation
 - d. Drag the timeline to scrub through the animation
 - e.



Attend a Quiz

1. At the topic page (<http://serverIPaddress:3001/attendTopic/TopicID>)
2. Click on the “Attend Quiz” button.



3. Choose the answers and submit.

The screenshot shows the CryptBase interface. On the left is a dark sidebar with the user's name 'Wu ChuJun', a search bar, and links to 'Home' and 'Profile'. The main area is titled 'Quiz (Topic ID: CT001)'. A blue 'Submit' button is highlighted with a red box and a red '2'. Below it, two questions are listed, each with four radio button options. The first question is 'Question 1: Who is the creator of Trapdoor Knapsack Cryptosystems?' with options A. Merkle and Hellman (selected), B. Diffie and Hellman, C. Shannon, and D. Japit. The second question is 'Question 2: Trapdoor Knapsack makes use of a difficult problem. What is it?' with options A. Riemann Hypothesis, B. Subset Sum Problem (selected), C. P vs. NP Problem, and D. Navier-Stokes Equation. A red '1' is next to the second question's options.

CryptBase

Wu ChuJun

Search...

Home

Profile

Quiz (Topic ID: CT001)

Submit 2

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. 1

4. Done.

The screenshot shows the same CryptBase interface, but the quiz questions are no longer visible. Instead, a message at the bottom of the main area reads 'Congrats! You have completed the quiz! Your score is 2'. The 'Submit' button is still present. The sidebar and header remain the same.

CryptBase

Wu ChuJun

Search...

Home

Profile

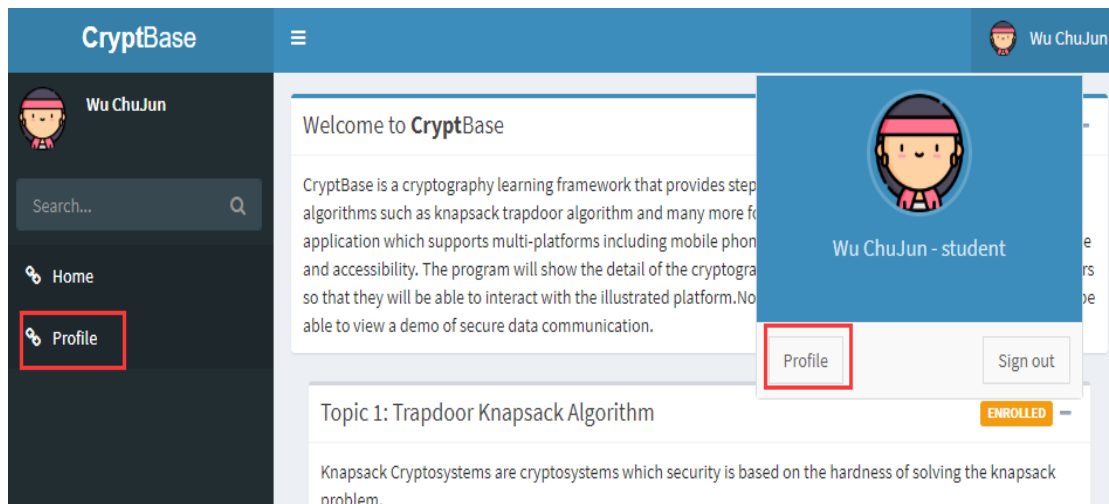
Quiz (Topic ID: CT001)

Submit

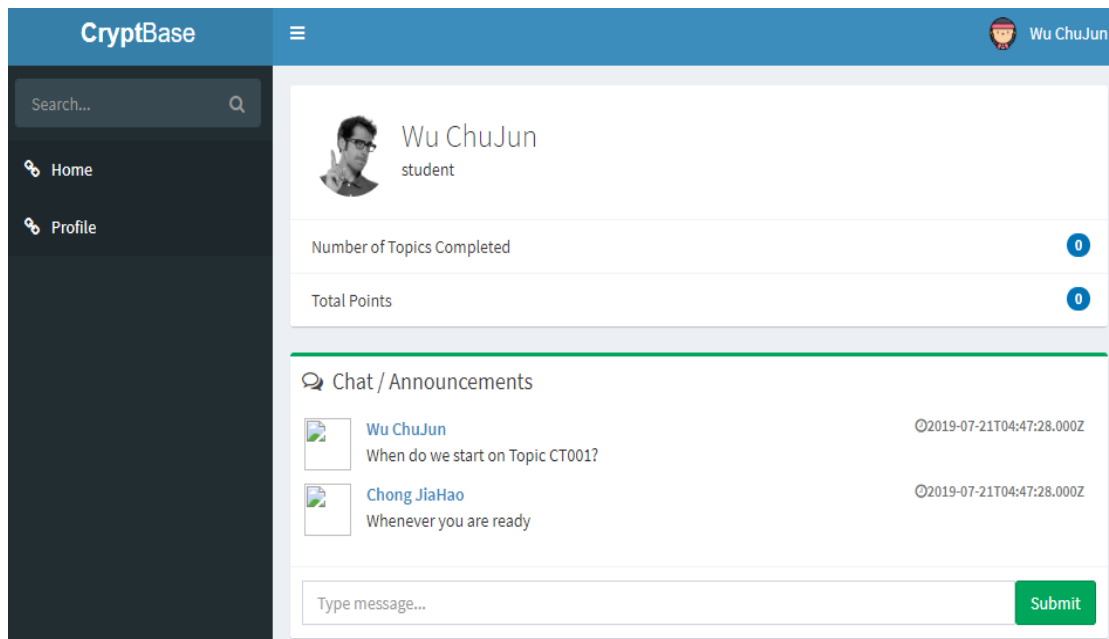
Congrats! You have completed the quiz!
Your score is 2

View Profile

1. Access Profile Page by using left-hand menu or top right corner button.



2. Done.



Lecturer

Manage Topics

CryptBase

Chong JiaHao

Search...

Manage Topic

Profile

Manage Topics

Create New Topic

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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
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

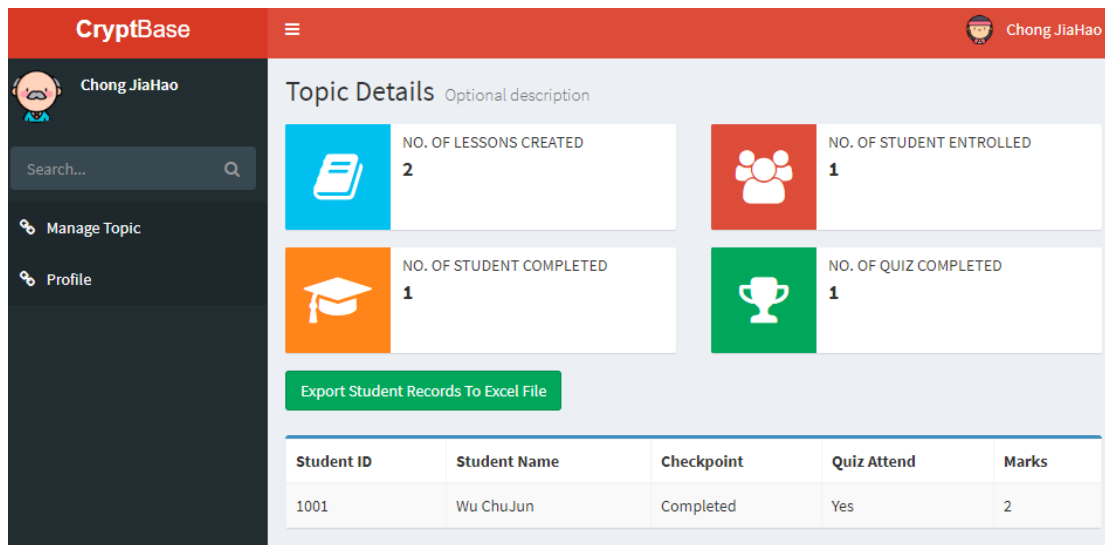
*Only owner of the topic will able to manage it

Topic Overview

1. Click on the "Overview" Button

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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>

2. Done



CryptBase Chong JiaHao

Topic Details Optional description

NO. OF LESSONS CREATED: 2

NO. OF STUDENT ENROLLED: 1

NO. OF STUDENT COMPLETED: 1

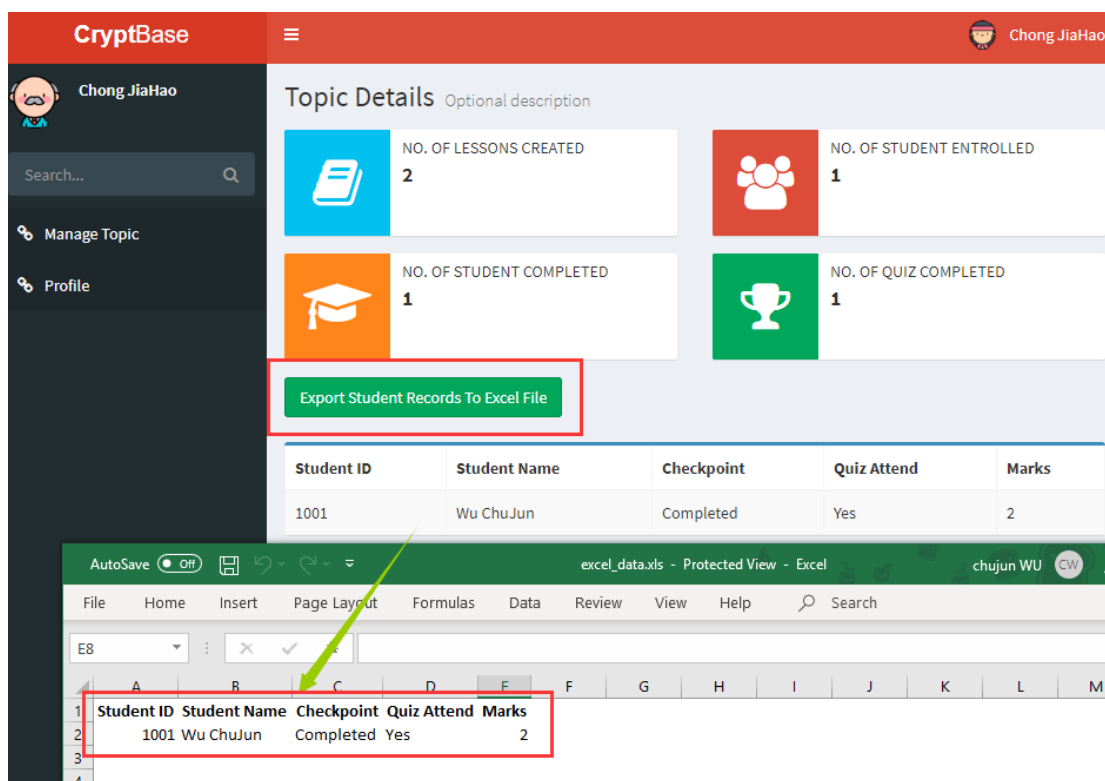
NO. OF QUIZ COMPLETED: 1

Export Student Records To Excel File

Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1001	Wu ChuJun	Completed	Yes	2

Export Student Records

1. Click on the “Export Student Records To Excel File” button.
2. Done.



CryptBase Chong JiaHao

Topic Details Optional description

NO. OF LESSONS CREATED: 2

NO. OF STUDENT ENROLLED: 1

NO. OF STUDENT COMPLETED: 1

NO. OF QUIZ COMPLETED: 1

Export Student Records To Excel File

Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1001	Wu ChuJun	Completed	Yes	2

excel_data.xls - Protected View - Excel chujun WU

File Home Insert Page Layout Formulas Data Review View Help Search

E8

Student ID	Student Name	Checkpoint	Quiz Attend	Marks
1001	Wu ChuJun	Completed	Yes	2

Create New Topic

1. At the Manage Topic Page ([http:// serverIPaddress:3001/manageTopic](http://serverIPaddress:3001/manageTopic))
2. Click on “Create New Topic”

CryptBase

Chong JiaHao

Search...

Manage Topic

Profile

Manage Topics

Create New Topic

Topic ID	Topic Name	Description
CT001	Trapdoor Knapsack Algorithm	Knapsack Cryptosystems are cryptosystems wh security is based on the hardness of solving the problem.

3. Fill in all the details and click on “Save changes”.

Create Topic With Information

Topic ID

CT003

Topic Name

TOPIC 3

Description

THIS IS A TEST

Close

Save changes

4. Close the window and refresh the page.

CryptBase

Chong JiaHao

Search...

Manage Topic

Profile

Manage Topics

Create New Topic

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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
CT003	TOPIC 3	THIS IS A TEST	Chong JiaHao	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
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

Update Topic Information

1. At the Manage Topic Page ([http:// serverIPaddress:3001/manageTopic](http://serverIPaddress:3001/manageTopic))
2. Click on “Update Info” button

CT003	TOPIC 3	THIS IS A TEST	Chong JiaHao	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
-------	---------	----------------	--------------	--

3. Fill in the new details and click on “Save changes”

Update Topic Information for CT003

Topic Name

TOPIC 99999999

Description

I AM A TEST :)

Close

Save changes

4. Close the window and refresh the page.

CryptBase		Chong JiaHao		
Manage Topics		Create New Topic		
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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
CT003	TOPIC 99999999	I AM A TEST :)	Chong JiaHao	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>
Updated				
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

Manage Lessons

1. At the Manage Topic Page ([http:// serverIPaddress:3001/manageTopic](http://serverIPaddress:3001/manageTopic))
2. Click on “Lesson”

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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>

Create a HTML Lesson

1. Click on “Create New Lesson (HTML)”

Manage Lesson (CT001)

🏠 Level > Here

Upload A File as Lesson

Create New Lesson (HTML)

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 given limit and the total value is as large as possible	Html	<div>View Page</div> <div>Update</div>
2	What is Trapdoor	A trapdoor is a piece of knowledge which makes it easier to find X from $f(X)$	Html	<div>View Page</div> <div>Update</div>

2. Fill in the contents and click on the “Save changes” button

CryptBase

Wu ChuJun

Search...

Home

Profile

CT001: Trapdoor Knapsack Algorithm

Attend Quiz

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 given limit and the total value is as large as possible

START

Lesson 2: What is Trapdoor

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

START

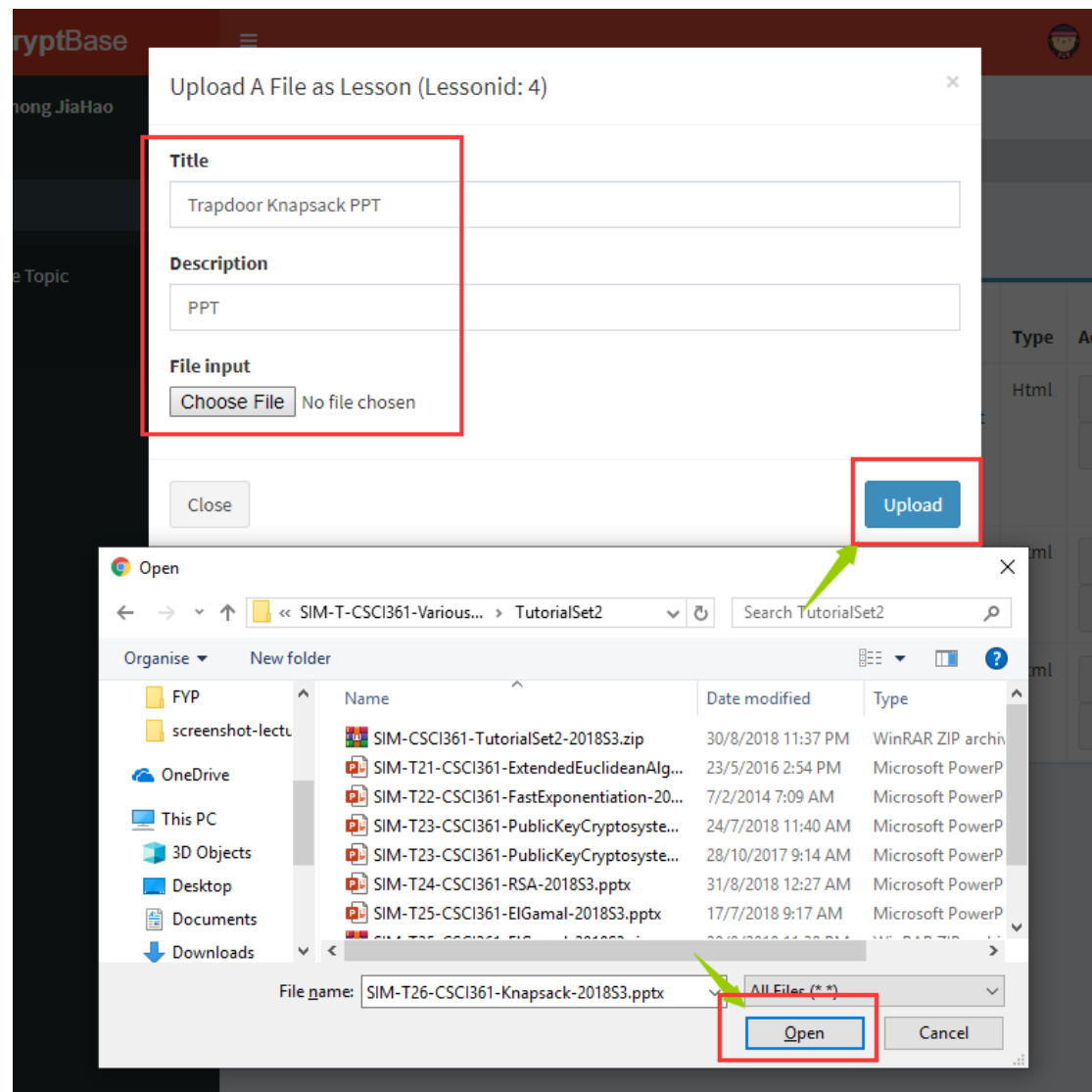
Lesson 3: Test Lesson 3

I am a test

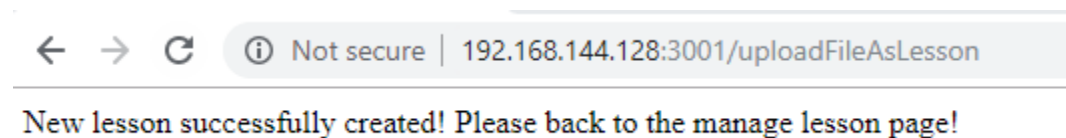
START

Upload a file as lesson

1. Click on the “Upload file as a lesson”
2. Fill in the contents, select the file and upload



3. Upload successfully



4. Refresh the page and Download the file if needed

Chong JiaHao

File Home Insert Design Transition Animation Slide Review View Help Search

Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View. [Enable Editing](#)

TUTORIAL 2

CSCI361 – Computer Security

Sionggo Japit
sjapit@uow.edu.au
20 August 2019

Slide 1 of 16 Notes

Lesson ID	Lesson Title	File Type	Actions
1			View Page Update
2			View Page Update
3	Test Lesson 3	Html	View Page Update
4	Trapdoor Knapsack PPT	File	Download Update

CryptBase

Wu ChuJun

Search...

[Home](#)
[Profile](#)

Trapdoor Knapsack PPT

Description:
PPT

Contents:

[Download Lesson File](#)

[<< Previous Lesson](#)

Manage Quiz

1. At the Manage Topic Page ([http:// serverIPaddress:3001/manageTopic](http://serverIPaddress:3001/manageTopic))
2. Click on “Quiz”

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	<div>Overview</div> <div>Lesson</div> <div>Update Info</div> <div>Quiz</div>

Add quiz question

1. Click on the button

Add Quiz Question

Quiz ID	Question	Answers	Right Answer	Action
undefined Please create quiz first				

2. Fill in the details and Click on the “Save changes”
3. Done.

Quiz (Topic ID: CT003)

👤 Level > Here

Add Quiz Question

Quiz ID	Question	Answers	Right Answer	Action
1	here is a test	<ul style="list-style-type: none">test1test2test3test4	test4	<div>Update</div>

Change a quiz question

1. Click on the “Update” button

Add Quiz Question				
Quiz ID	Question	Answers	Right Answer	Action
1	here is a test	<ul style="list-style-type: none">• test1• test2• test3• test4	test4	<div>Update</div>

2. Fill in the new details and Click on the “Save changes”
3. Refresh the page

Quiz ID	Question	Answers	Right Answer	Action
1	here is a test	<ul style="list-style-type: none">• test1• test2• test3• test4555	test4555	<div>Update</div>