

IEMS5710B Crypto., Info. Security and Privacy (2<sup>nd</sup> Trimester, 2023-24)  
Laboratory Assignment: Experiencing Security-related Computing Environments  
Due date: Dec 19<sup>th</sup>, 2023, 11:59 pm HK Time. Submission: <http://blackboard.cuhk.edu.hk>

## Objectives

This “laboratory assignment” covers some selected topics we will cover in the lectures. Upon completion, you will be able to:

- Establish a secure communication channel using public-key encryption
- Change the access level of a file in a Linux machine
- Write some simple SQL queries for querying a database
- Write an HTML webpage file to interact with a “web application” written in PHP

(This assignment aims to give you first-hand experiences in related computing environments. You are advised to finish at least the first three parts of the question early to have some hands-on experience before you commit to taking this course.)

## Q1. Encryption and Decryption using GPG4WIN

### I. Installation

1. Download GPG4WIN from the following URL: <https://www.gpg4win.org/download.html>
2. Click the download button.

#### Gpg4win 4.2.0 (Released: 2023-07-14)

You can download the full version (including the Gpg4win compendium) of Gpg4win 4.2.0 here:

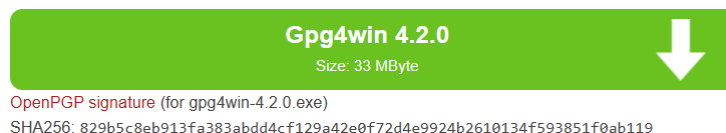


Figure 1

3. Select “\$0” and start to download. // Well, you can always choose to donate :)



Figure 2

4. Double-click the file to start the installation process.
5. Select the default option.

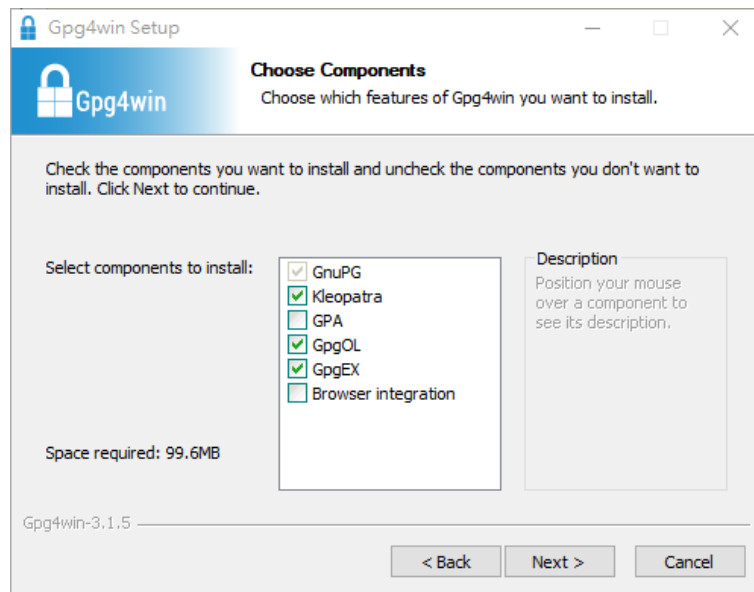


Figure 1

6. Finally, select Run Kleopatra and press **Finish**.



Figure 4

## II. Generate a public and private key pair

This section demonstrates the steps to generate a public and private key pair in the system.

1. After the software has started, select the **New OpenPGP Key Pair** option.  
(Question you should ask yourself: What does “PGP” stand for? Google is your friend.)

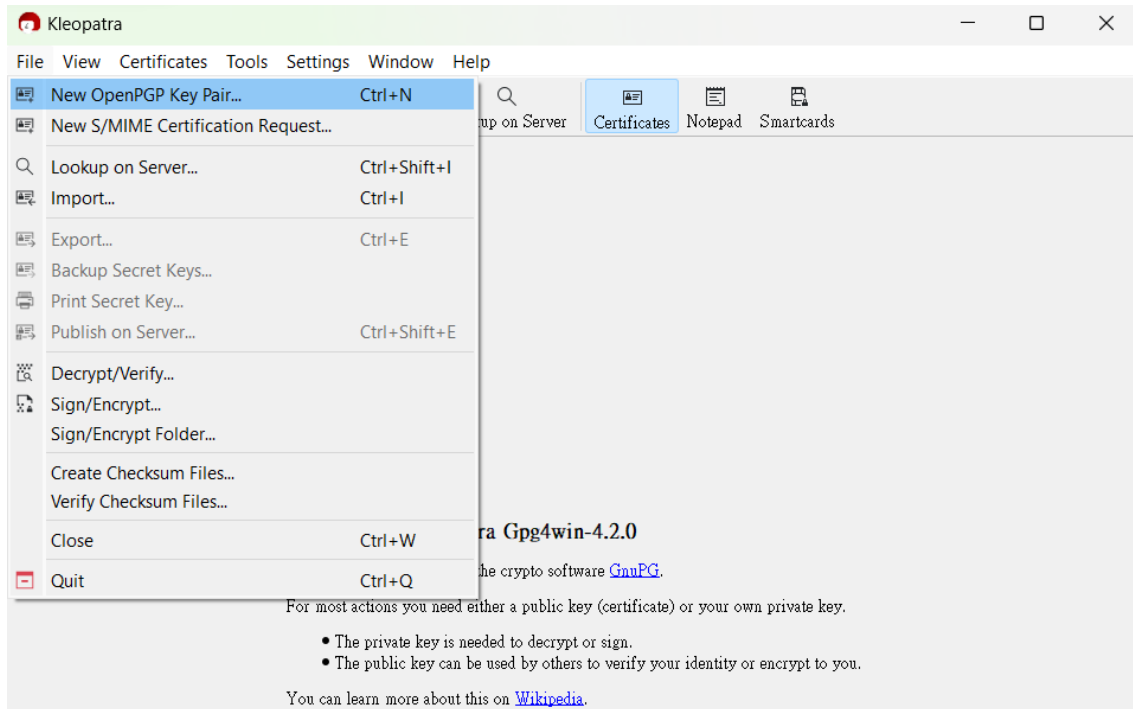


Figure 5

2. Select **Create a personal OpenPGP key pair**, fill in your name and email address if you want, and tick the box “Protect the generated key with a passphrase.”

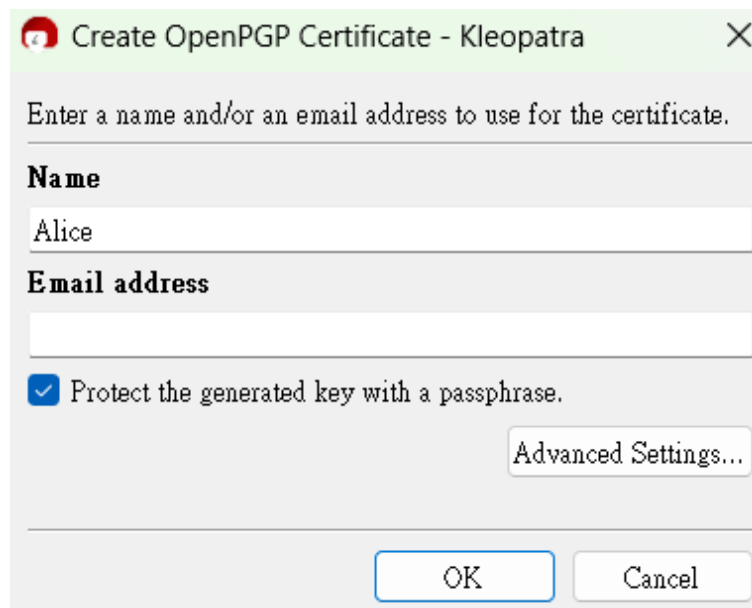


Figure 6

You can click **Advanced Settings** for other available options. For example, you can increase the key length in the advanced setting dialog box. We will use the default options in this lab assignment. (Question to yourself: What are ECDSA, EdDSA, ed25519, and ECDH?)

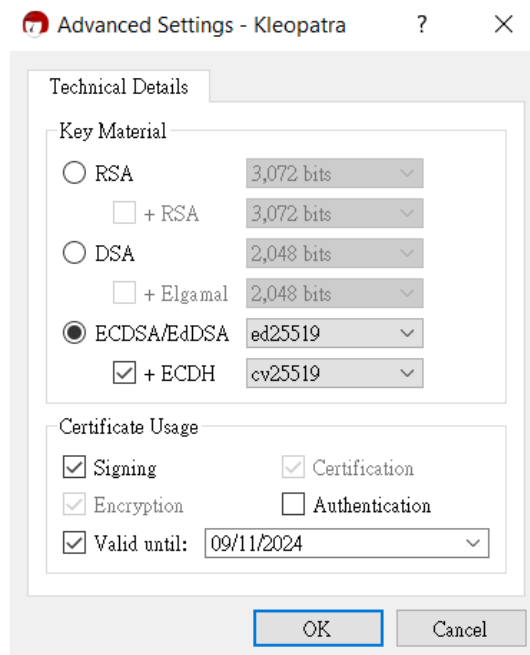


Figure 7

3. Click the **OK** button to create the key pair.
4. Enter a password to protect your new (private) key.

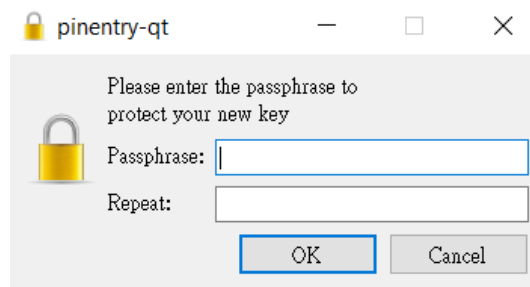


Figure 8

5. Your new key pair has been created.

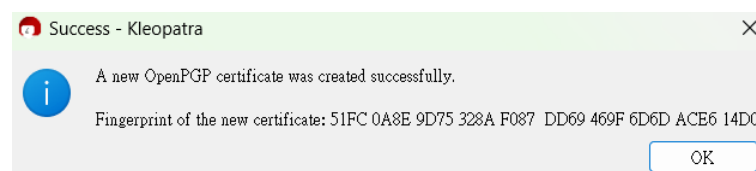


Figure 9

6. Click **Finish** to exit the dialog box.

### III. Export your own public key

To establish a secure communication channel, you have to give your public key to others. This section details the steps to export your public key to a file so you can send it out.

1. After you press “Finish” in the previous step, you will see the following box.

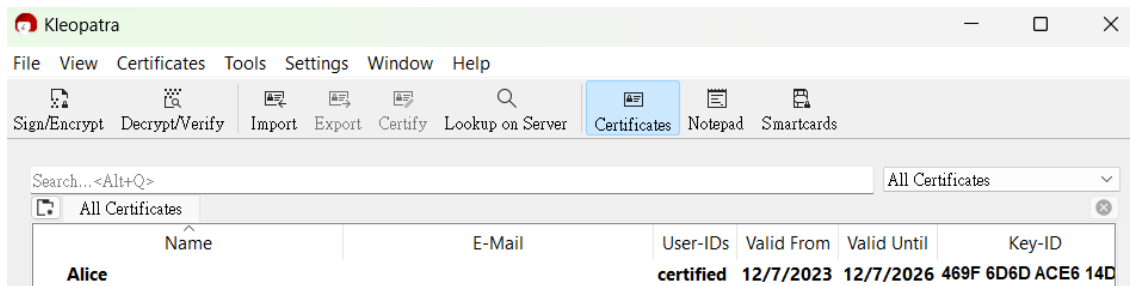


Figure 10

2. Move your mouse cursor and double-click your name.
3. The certificate details will be shown.

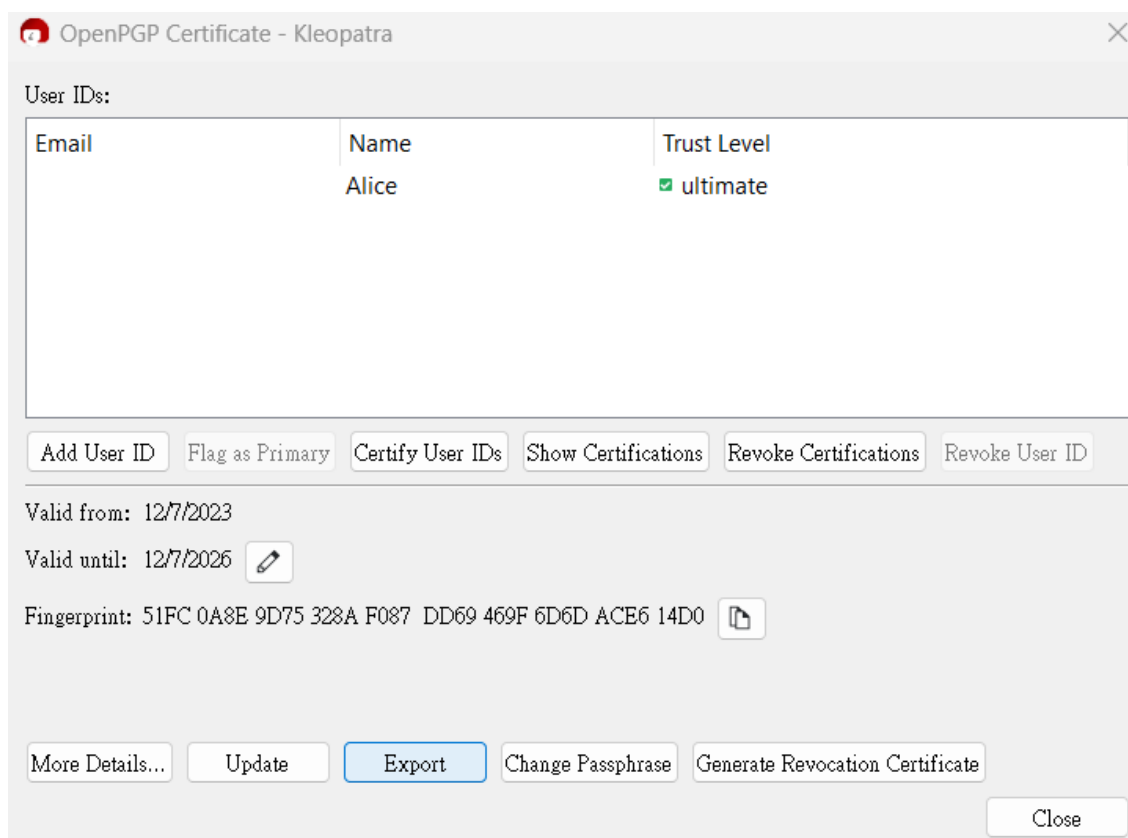
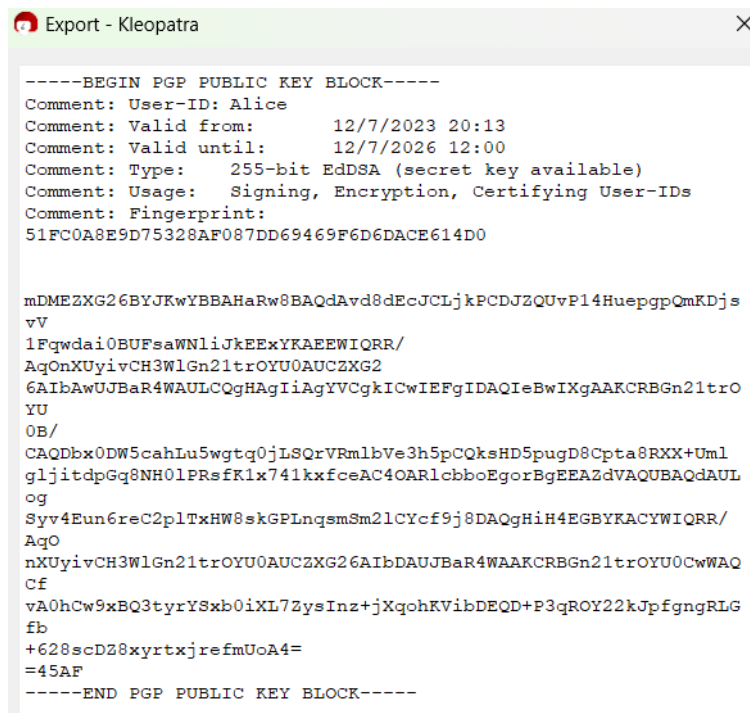


Figure 11

4. Click the **Export** button to view your public key.



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID: Alice
Comment: Valid from:      12/7/2023 20:13
Comment: Valid until:    12/7/2026 12:00
Comment: Type:           255-bit EdDSA (secret key available)
Comment: Usage:          Signing, Encryption, Certifying User-IDs
Comment: Fingerprint:
51FC0A8E9D75328AF087DD69469F6D6DACE614D0

mDMEZXG26BYJKwYBBAHaRw8BAQdAvd8dEcJCLjkPCDJZQUvP14HuepgpQmKDjs
vV
1Fqwdai0BUFSaWNliJkEEeYKAEEWIQRR/
AqOnXUYivCH3WlGn21trOYU0AUCZXG2
6AIbAwUJBar4WAULCQgHAgIiAgYVCgkICwIEFgIDAQIEBwIXgAAKCRBGn21trO
YU
0B/
CAQDbx0DW5cahLu5wgtq0jLSQrVRmlbVe3h5pCQksHD5pugD8Cpta8RXX+Uml
gljitdpGq8NH01PRsfK1x741kxfceAC4OARlcbboEgorBgEEAZdVAQUBAQDAUL
og
Syy4Eun6reC2plTxHW8skGPLnqsmSm2lCYcf9j8DAQgHiH4EGBYKACYWIQRR/
AqO
nXUYivCH3WlGn21trOYU0AUCZXG26AIbDAUJBar4WAAKCRBGn21trOYU0CwWAQ
Cf
vA0hCw9xBQ3tyrYSxb0iXL7ZysInz+jXqohKVibDEQD+P3qROY22kJpfgngRLG
fb
+628scDZ8xyrtxjrefmUoA4=
=45AF
-----END PGP PUBLIC KEY BLOCK-----
```

Figure 12

5. Right-click and select all content. Copy the content to the clipboard. Open a text editor (e.g., notepad) and paste the content. Remove lines 2 to 9 from the content. You should have the following screen.



```
Alice_public_key.txt x
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2 mDMEZXG26BYJKwYBBAHaRw8BAQdAvd8dEcJCLjkPCDJZQUvP14HuepgpQmKDjsvV
3 1Fqwdai0BUFSaWNliJkEEeYKAEEWIQRR/AqOnXUYivCH3WlGn21trOYU0AUCZXG2
4 6AIbAwUJBar4WAULCQgHAgIiAgYVCgkICwIEFgIDAQIEBwIXgAAKCRBGn21trOYU
5 0B/CAQDbx0DW5cahLu5wgtq0jLSQrVRmlbVe3h5pCQksHD5pugD8Cpta8RXX+Uml
6 gljitdpGq8NH01PRsfK1x741kxfceAC4OARlcbboEgorBgEEAZdVAQUBAQDAULog
7 Syy4Eun6reC2plTxHW8skGPLnqsmSm2lCYcf9j8DAQgHiH4EGBYKACYWIQRR/AqO
8 nXUYivCH3WlGn21trOYU0AUCZXG26AIbDAUJBar4WAAKCRBGn21trOYU0CwWAQCf
9 vA0hCw9xBQ3tyrYSxb0iXL7ZysInz+jXqohKVibDEQD+P3qROY22kJpfgngRLGfb
10 +628scDZ8xyrtxjrefmUoA4=
11 =45AF
12 -----END PGP PUBLIC KEY BLOCK-----
```

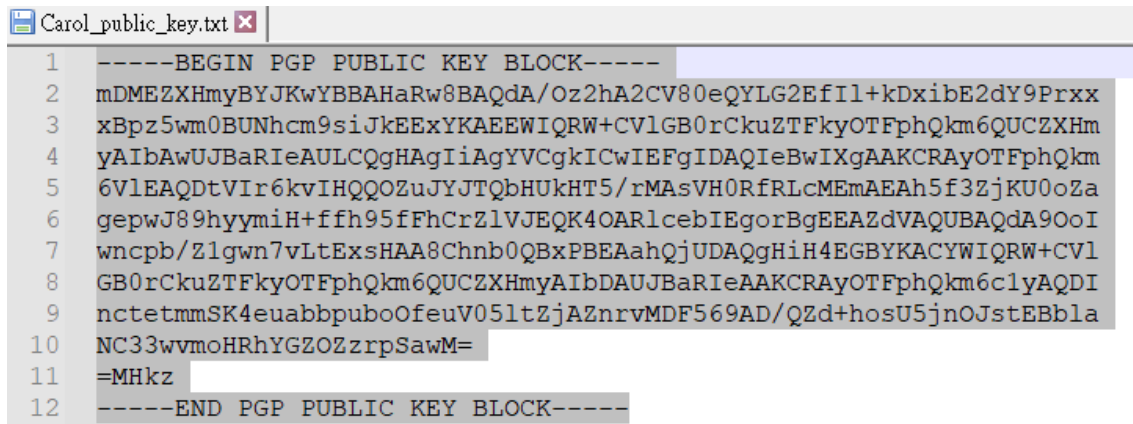
Figure 13

6. Save the file and name it **[your name]\_public\_key.txt**.
7. You can send this file to your partner for the following step.

#### IV. Import others' public keys.

You need other's public key to encrypt messages for secure communication. This section demonstrates the steps to import others' public keys into the system.

1. When you obtain the public key from others, open it with a text editor and copy the content to the clipboard.



```
Carol_public_key.txt
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2 mDMEZXHmyBYJKwYBBAHaRw8BAQdA/Oz2hA2CV80eQYLG2EfI1+kDxibE2dY9Prxx
3 xBpz5wm0BUNhcm9siJkEEExYKAEEWIQRW+CVlGB0rCkuZTFkyOTFphQkm6QUCZXHm
4 yAIbAwUJBarIeAULCQgHAgIiAgYVCgkICwIEFgIDAQIeBwIXgAAKCRAyOTFphQkm
5 6VlEAQDtVlr6kvIHQQOZuJYJTQbHUKHT5/rMAsVH0RfRLcMEMAEAh5f3ZjKU0oZa
6 gepwJ89hyymiH+ffh95fFhCrZlVJEQK4OARlcebIEgorBgEEAZdVAQUBAQdA90oI
7 wncpb/Zlgnw7vLteXsHAA8Chnb0QBxPBEAahQjUDAQgHiH4EGBYKACYWIQRW+CVl
8 GB0rCkuZTFkyOTFphQkm6QUCZXHmyAIbDAUJBarIeAAKCRAyOTFphQkm6c1yAQDI
9 nctetmmSK4euabbpuboOfeuV051tZjAZnrVMDf569AD/Qzd+hosU5jnOJstEBbla
10 NC33wvmoHRhYGZOZzrpSawM=
11 =MHkz
12 -----END PGP PUBLIC KEY BLOCK-----
```

Figure 14

2. Go to Kleopatra and select **Certificate Import** (the button is grey if nothing is copied).

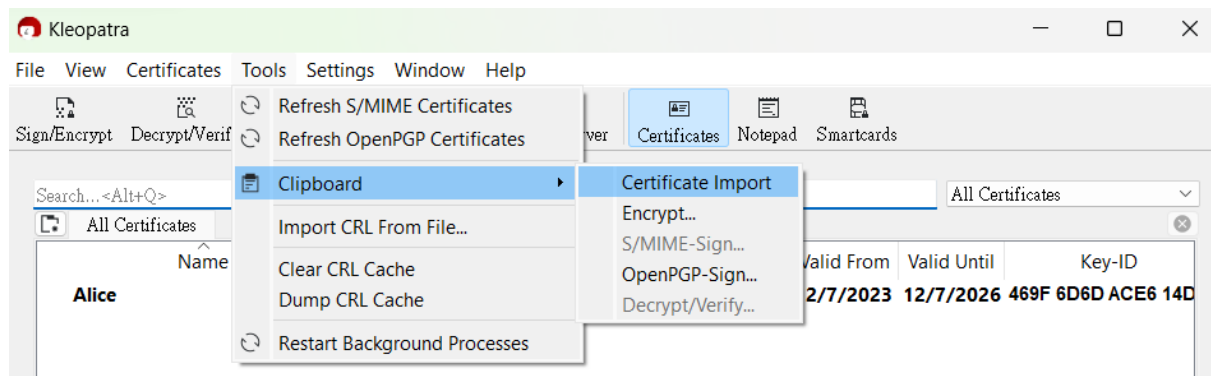


Figure 15

3. In this dialog box, click **Certify**.

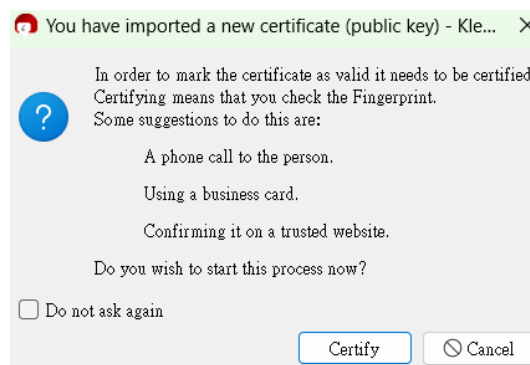


Figure 16

4. Click **Certify**.



Figure 17

5. Input the password that you have set in Section II.

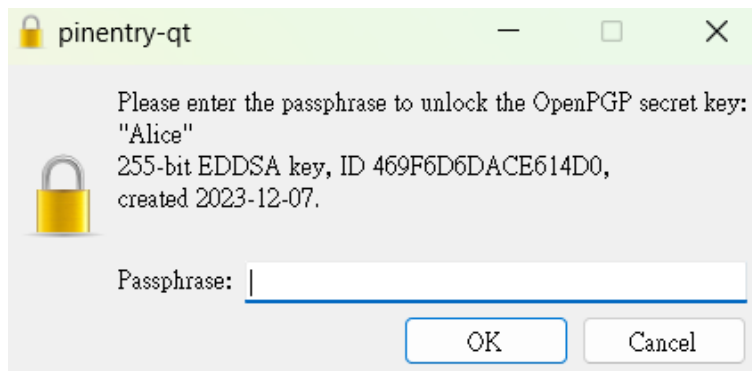


Figure 18

6. The public key of Carol has been imported successfully.

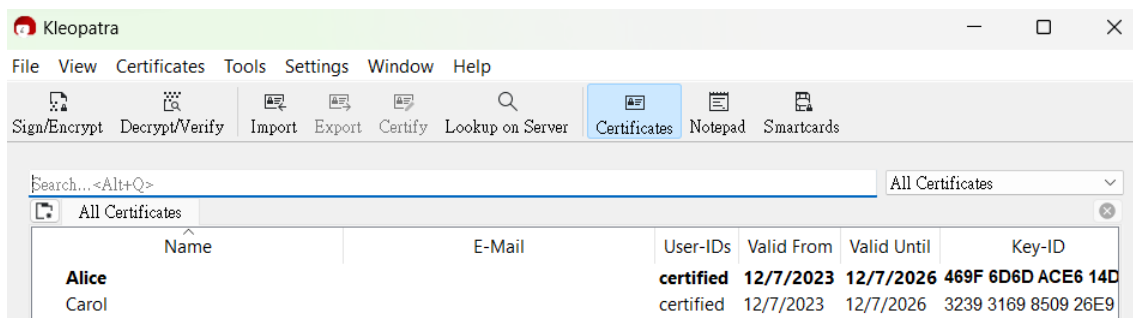


Figure 19



## V. Encrypt messages by using the public key and sign by using your private key

After you have imported other's public key to the system, you can use his/her public key to encrypt a message and use your own private key to sign the message. This section demonstrates the steps to do so.

1. Open Kleopatra and select the **Notepad** button in the toolbar.

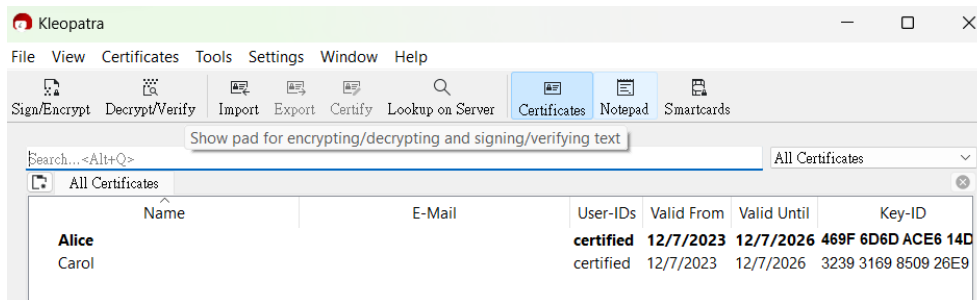


Figure 20

2. Type in the message that you are going to encrypt.

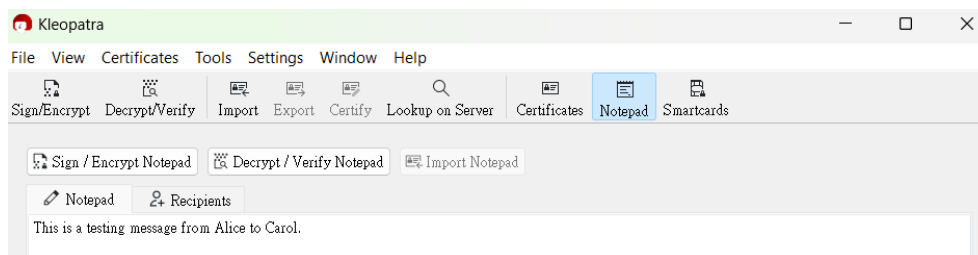


Figure 21

3. In the **Recipients** tab, tick the **Sign as** option and input the recipient's name in the **Encrypt for others** section; click the **Sign/Encrypt Notepad** button.

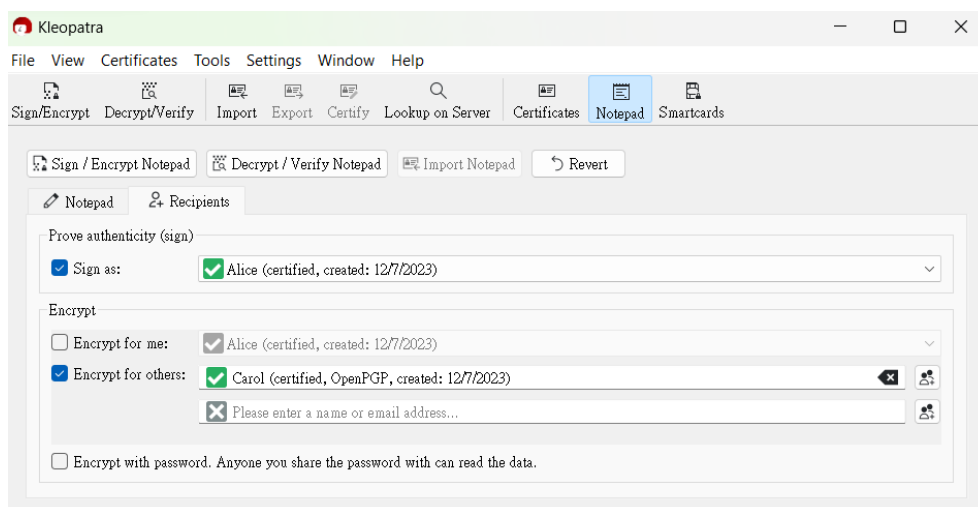


Figure 22

4. The encryption is done successfully.

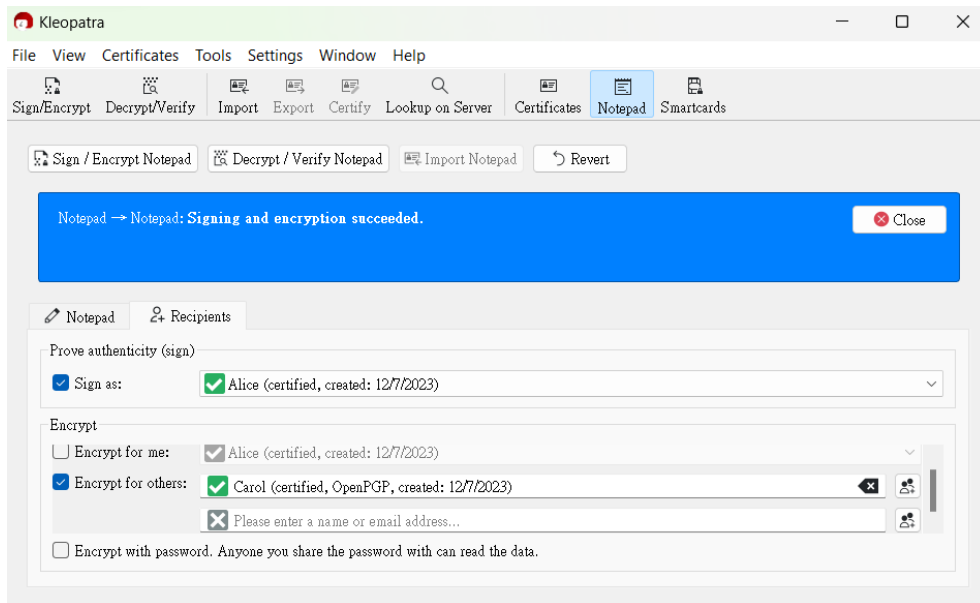


Figure 23

5. Select the **Notepad** tab, and you can view the encrypted message.

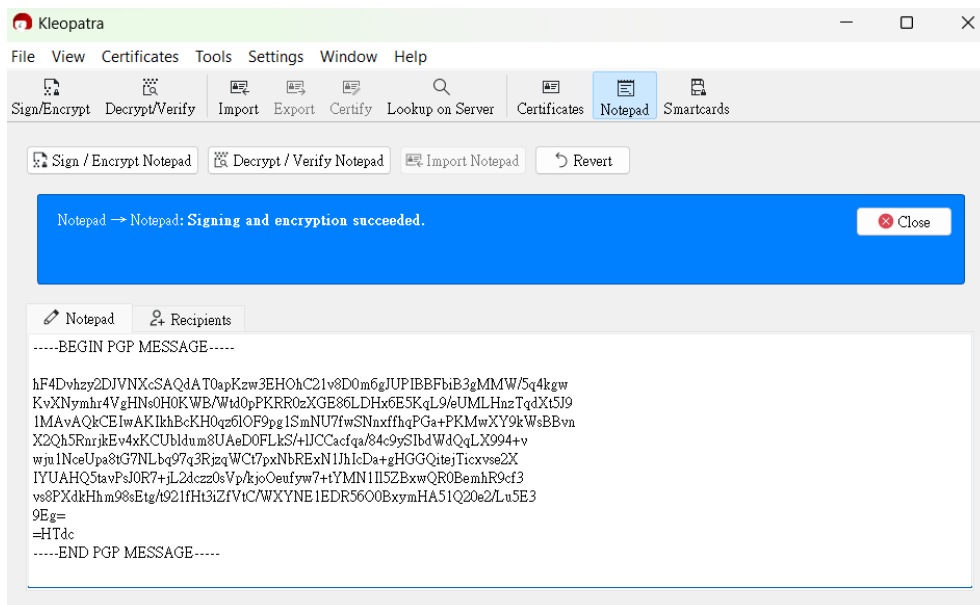


Figure 24

6. You can copy and send the content as a file or by email.

VI. Decrypt message by using the private key and verify using other's public key  
 After receiving the encrypted message from the sender, you can use your private key to decrypt the message and use sender's public key to verify the sender identity.

1. On the recipient's side, open Kleopatra and click the **Notepad** button.

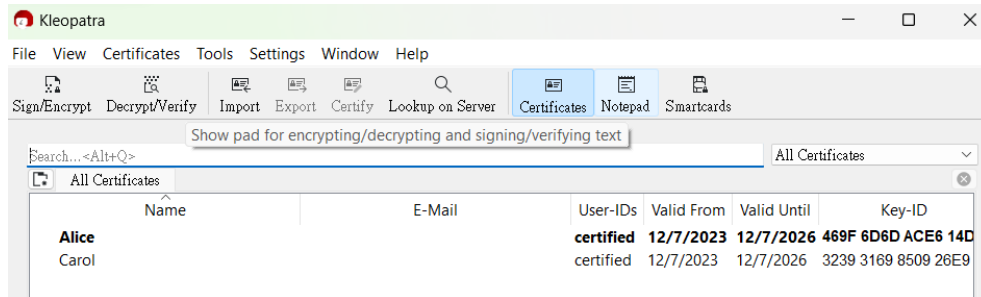


Figure 25

2. In the **Notepad** tab, paste the encrypted message to the box and click the **Decrypt/Verify Notepad** button.

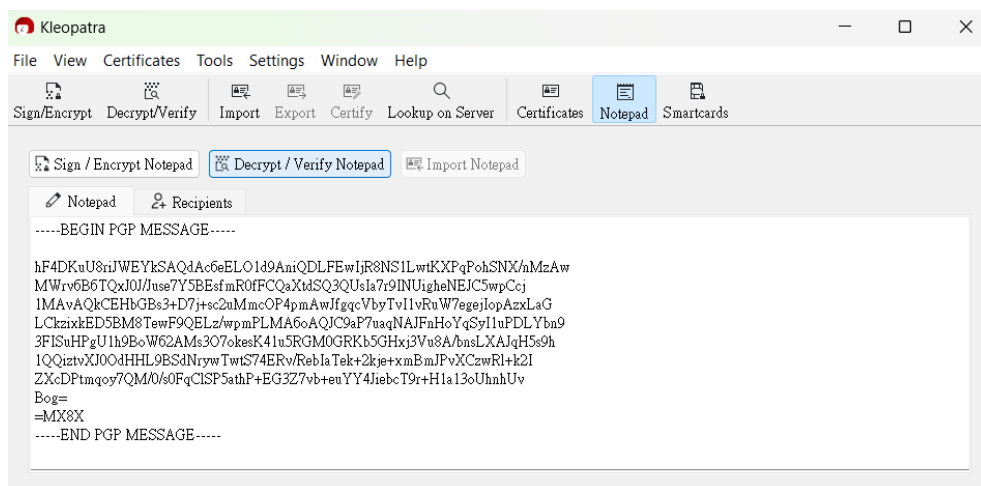


Figure 26

3. Kleopatra will verify the sender's identity and start decrypting the content.

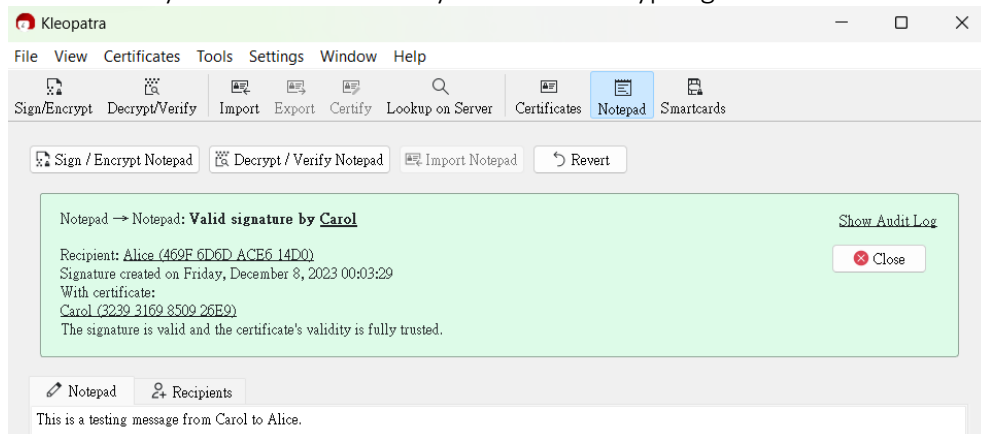


Figure 27

## VII. Your tasks

In this question, you need to submit the following:

1. Generate a public and private key pair (Figure 9).
2. Export your public key to a file (Figure 12).
3. Import your partner's public key to the system (Figure 19).
4. Encrypt a message to your partner (Figure 24).
5. Decrypt an encrypted message from your partner (Figure 27).

To show your work, you need to capture your computer screen in each step (*i.e.*, **Figures 9, 12, 19, 24, and 27**) and include them in your report.

Optionally, you can include the long form of the acronyms you encountered.

## Q2. Access Control in Linux Machine

### I. Connect to a Linux VM

1. Go to the following URL: <https://cocalc.com/doc/terminal.html>.
2. Sign up for an account and click **Your CoCalc projects** to start an Online Linux Terminal.

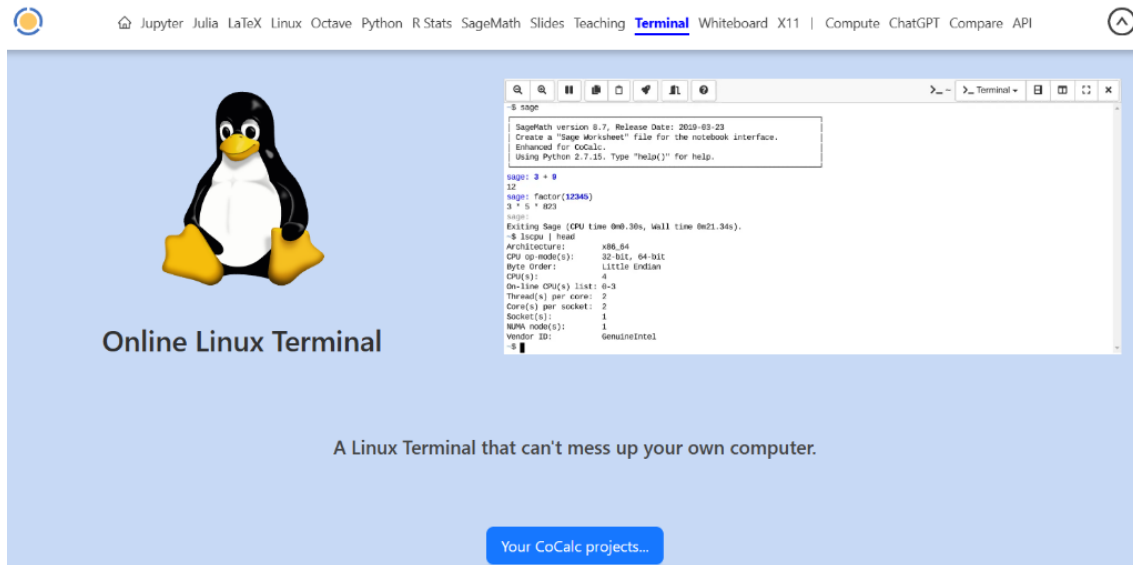


Figure 28

### II. Create a new project

1. Click **Create Project**, type the project name and click **Create Project** again.

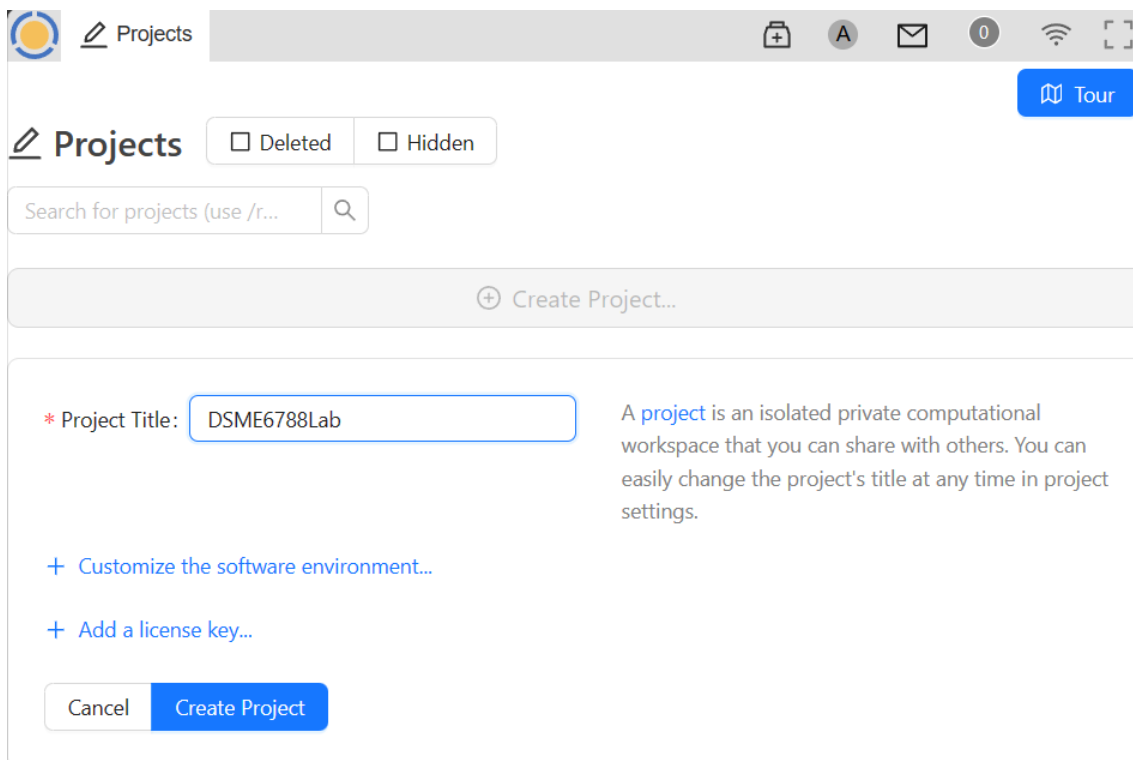


Figure 29

2. Click **Start Project** and type command in **Terminal command**.

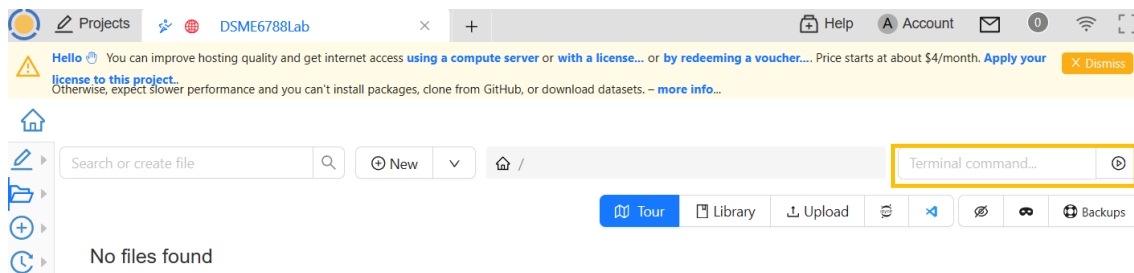


Figure 30

### III. Create a sample file

1. Type the following command in the shell and press enter to execute it:

```
echo "This is a test file" > test_1.txt
```

`echo` is a command for displaying something on the console display.

`>` is a symbol for redirecting from the console display.

`test_1.txt` will be the destination for the above redirection.

Simply put, the effect is it will create a file called `test_1.txt` with one line.  
Warning: it **OVERWRITES** the file if the file exists.

2. Execute the following command to list the file in the current directory:

```
ls -l
```

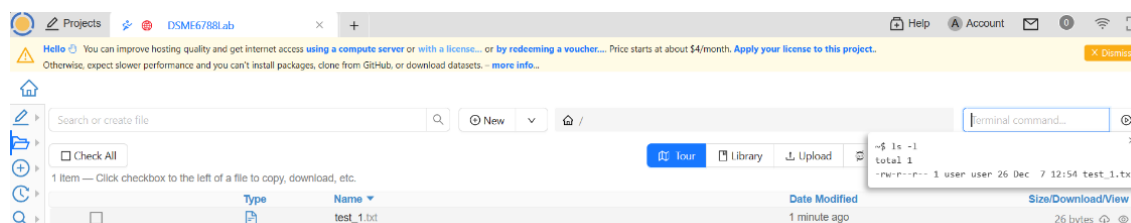


Figure 31

`ls` is a command for listing directory (folder in Windows terminology) contents.

`ls -l` means "using a long listing format."

You can try `ls --help` or `man ls` to know more about `ls`.

#### IV. Set the access level of a file in a Linux machine

1. In Linux, we use the **chmod** command with the following syntax to set/change the access level of a file:

```
chmod [option] permissions file_name
```

There are three kinds of users:

**u** = owner

**g** = the group where the file belongs to

**o** = others

Also, there are three kinds of access restrictions:

**r** = 4 = read

**w** = 2 = write

**x** = 1 = execute

Here, *option* is not necessary to set.

2. To **add** the **executing** permission of **test\_1.txt** to the **owner**, we execute the following:

```
chmod u+x test_1.txt
```

3. To **remove** the **reading** permission of **test\_1.txt** the **group of users** and **others**:

```
chmod g-r,o-r test_1.txt
```

4. To **add** the **reading**, **writing**, and **executing** permission to **owner**, **group of users**, and **others**:

```
chmod u+wrx,g+rwx,o+rwx test_1.txt
```

The above command is equivalent to the above command:

```
chmod 777 test_1.txt
```

Here 7 equals **wrx** (4+2+1).

#### V. Your tasks

In this question, you need to submit the commands to do the following:

1. Create a file named **[the last 4 digits of your SID].txt** with **"Submission to Q2"** as content.
2. Set the following access restriction of the above file to different users:
  - a. Give the reading, writing, and executing permission to the owner.
  - b. Give the reading and executing permission to group of users.
  - c. Give the executing permission to others.
  - d. Submit both commands using alphabetical and numerical representations of the permission restriction.

### Q3. Basic SQL

#### I. Connect to the SQL Online IDE

Go to the following URL:

<https://sqliteonline.com>

To run a query, just click **Run** or press **Shift + Enter**.

#### II. Learn SQL

Structured Query Language (SQL) is a database query language that allows the management of data in a relational database. In this part, we provide some basic SQL query examples to give you a taste of how they work, which helps you better understand the SQL injection to be covered in the lecture later.

1. **CREATE** a table name `users_info` which is constructed by three columns: `ID` (unique int), `username` (varchar(225)), `password` (varchar(225)):

```
CREATE TABLE users_info (  
    ID INT NOT NULL UNIQUE,  
    username VARCHAR(225) NOT NULL,  
    password VARCHAR(225) NOT NULL  
);
```

Once a table is created, it cannot be created again; hence, the above query can be run only once.

To **DELETE** the table, we use **DROP**:

```
DROP TABLE users_info;
```

A query ends with “;”.

2. **INSERT** the following rows into `user_info`:

```
INSERT INTO users_info (ID, username, password)  
VALUES (1, 'Alice', '123456'),  
(2, 'Bob', 'password'),  
(3, 'Carol', '1password'),  
(4, 'Dave', 'abc123'),  
(5, 'Eve', 'qwerty'),  
(6, 'Alice', '111111');
```



3. **SELECT** all columns of users\_info:

```
SELECT * FROM users_info;
```

You should see the following output:

ID	username	password
1	Alice	123456
2	Bob	password
3	Carol	1password
4	Dave	abc123
5	Eve	qwerty
6	Alice	111111

Figure 32

4. Select specific columns from users\_info:

```
SELECT ID, username FROM users_info;
```

ID	username
1	Alice
2	Bob
3	Carol
4	Dave
5	Eve
6	Alice

Figure 33

5. Use the **WHERE** clause to filter some of the records:

```
SELECT * FROM users_info WHERE ID=1;
```

ID	username	password
1	Alice	123456

Figure 34

6. Use the **LIKE** operator to search for records containing a specific pattern:

Username starts with "a":

```
SELECT * FROM users_info WHERE username LIKE "a%";
```

ID	username	password
1	Alice	123456
6	Alice	111111

Figure 35

Username contains with "a":

```
SELECT * FROM users_info WHERE username LIKE "%a%";
```

ID	username	password
1	Alice	123456
3	Carol	1password
4	Dave	abc123
6	Alice	111111

Figure 36

Username ends with "e":

```
SELECT * FROM users_info WHERE username LIKE "%e";
```

ID	username	password
1	Alice	123456
4	Dave	abc123
5	Eve	qwerty
6	Alice	111111

Figure 37

7. Use the **BETWEEN** operator to select records given a range:

```
SELECT * FROM users_info WHERE ID BETWEEN 1 AND 3;
```

ID	username	password
1	Alice	123456
2	Bob	password
3	Carol	1password

Figure 38

8. Use **comparison** operators to select records given a condition:

They can be:

Operator	Description
=	Equal to
>	Greater than
<	Less than
>=	Greater than equal to
<=	Less than equal to
<>	Not equal to

Table 1

```
SELECT * FROM users_info WHERE ID > 3;
```

ID	username	password
4	Dave	abc123
5	Eve	qwerty
6	Alice	111111

Figure 39

9. Use **AND**, **OR** operator to select records based on more than one condition:

```
SELECT * FROM users_info WHERE ID BETWEEN 1 AND 2 OR username LIKE "%e";
```

ID	username	password
1	Alice	123456
2	Bob	password
4	Dave	abc123
5	Eve	qwerty
6	Alice	111111

Figure 40

10. Use **NOT** operator to select records that are not true for the given condition:

```
SELECT * FROM users_info WHERE ID NOT BETWEEN 1 AND 3;
```

ID	username	password
4	Dave	abc123
5	Eve	qwerty
6	Alice	111111

Figure 41

11. Create another table named **purchase\_record**, which contains the following columns with their corresponding data types: ID (int), item: (varchar(225)), date\_of\_purchase (date). Insert the following records into **purchase\_record**:

ID	item	date_of_purchase
1	cola	2023-11-01
1	shrimps	2023-11-02
3	orange juice	2022-03-10
4	chips	2021-04-10
5	chips	2022-12-02
5	apple	2022-12-02
5	lemon	2022-12-04

Figure 42

Try to write the query by yourself.

12. Use **ORDER BY** to sort the records based on some column(s); the default setting is in ascending order (ASC or DSEC to specify outputting in descending order):

```
SELECT * FROM purchase_record ORDER BY date_of_purchase;
```

ID	item	date_of_purchase
4	chips	2021-04-10
3	orange juice	2022-03-10
5	chips	2022-12-02
5	apple	2022-12-02
5	lemon	2022-12-04
1	cola	2023-11-01
1	shrimps	2023-11-02

Figure 43

13. Use a **JOIN** clause to combine the **ID** rows from **users\_info** and **purchase\_record**:

```
SELECT users_info.ID, users_info.username, purchase_record.item,  
purchase_record.date_of_purchase  
FROM users_info  
JOIN purchase_record ON users_info.ID = purchase_record.ID;
```

ID	username	item	date_of_purchase
1	Alice	cola	2023-11-01
1	Alice	shrimps	2023-11-02
3	Carol	orange juice	2022-03-10
4	Dave	chips	2021-04-10
5	Eve	chips	2022-12-02
5	Eve	apple	2022-12-02
5	Eve	lemon	2022-12-04

Figure 44

14. Use the **UNION** operator to combine the result of two or more **SELECT** statements:

```
SELECT ID FROM users_info
UNION
SELECT item FROM purchase_record;
```



ID
1
2
3
4
5
6
apple
chips
cola
lemon
orange juice
shrimps

Figure 45

## II. Your tasks

In this question, you need to do the following:

1. Create the table **users\_info** (Figure 32) and insert the records, which includes **an additional row**:  
ID: [the last 4 digits of your ID]  
username: [your nickname]  
password: [any password you like]
2. Create the table **purchase\_record** (Figure 42) and insert the records, which include **an additional row**:  
ID: [the last 4 digits of your ID]  
item: [anything you like]  
date\_of\_purchase: [the date you conduct this task]
3. Join **users\_info** and **purchase\_record** on their **ID**; select the **users\_info.ID**, **users\_info.username**, **purchase\_record.item**, **purchase\_record.date\_of\_purchase** with date of purchase after "2022-12-03" and order the records by date of purchase in descending order.

Submit the queries and the screenshot of the output.

## Q4. HTML

HTML stands for Hypertext Markup Language. It is the standard markup language for documents designed to be displayed in a web browser.

In this part, we will write some simple HTML to interact with a PHP file using an online editor.

### I. Start Coding with an Online Editor

1. Go to the following URL: <https://html.onlineviewer.net>.

The left part of this website is a coding platform that allows you to write your code, and the right part is a preview pane showing your code's result.

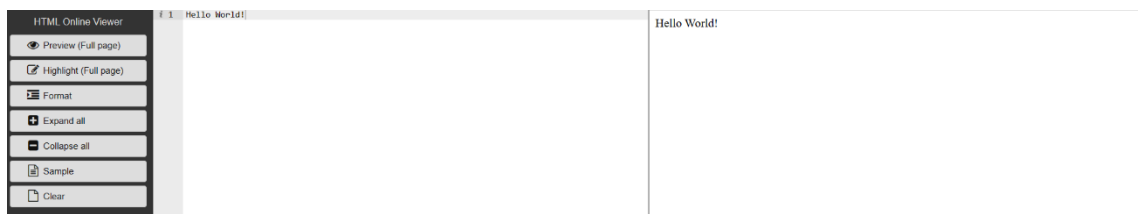


Figure 46

### II. HTML

We are going to write two HTML webpages, which submit your name and the last 4 digits of your SID to a “web file” written in PHP hosted at <https://iems5710.000webhostapp.com>.

In HTML, a tag (e.g., `<b></b>`) is used to tell the browser what the type of content is, and an element (e.g., `<b>12345</b>`) is used to tell the browser what to display. In this part, we use `<form>` element to collect the inputs and submit them to the hosted PHP file via the GET or POST method.

1. Copy and paste the following code on the coding platform (Figure 46):

```
<html>
<head>
  <style>
    header {
      font-family: Verdana;
      font-size: 20pt;
      font-weight: bold;
      margin-bottom: 20px;
    }
    body {
      font-family: Verdana;
      font-size: 14pt;
      margin: 40px;
    }
  </style>
</head>
```

```
<body>
<header>
  Please input the following information and click Submit
</header>
<form action="https://iems5710.000webhostapp.com" method="get">
Name: <input type="text" name="name"><br>
Last 4 digits of your SID: <input type="text" name="sid"><br>
<input type="submit">
</form>
</body>
</html>
```

Then, the webpage is shown on the right part:

## Please input the following information and click Submit

Name:

Last 4 digits of your SID:

Figure 47

2. Click **Preview (Full Page)** on the top-left to view the website in the full-page mode.
3. Input your **name** and **last 4 digits of your SID** on the boxes, then click the **Submit** button; you will see the following page:

```
Your request method is GET
Hi andes
Your last 4 digits of your SID: 5710
```

Figure 48

4. The above example uses the **GET** method to submit the request to the host. Now, let's modify the code to submit the request to the host via the **POST** method:

Change the following code in Step 1:

```
<form action="https://iems5710.000webhostapp.com" method="get">
```

To:

```
<form action="https://iems5710.000webhostapp.com" method="post">
```



### III. Your tasks

In this question, you need to do the following:

1. Do Steps 1-3 for submitting **GET** and **POST** requests.
2. Take the screenshots of Step 3 and include them in your report.
3. From the response pages of both HTML files, what are the differences between the **GET** and **POST** methods? (Hints: look at the URL of the response pages.)

### Assignment Submission

Put all screenshots, queries, and answers required in **Your tasks** of each question into a PDF file. Each question carries 25% of your total marks.

Please name the file in the following format:

***1155001234 Chan Tai Man.pdf***

Deadline: **Dec 19<sup>th</sup>, 2023, 11:59 pm Hong Kong Time.**