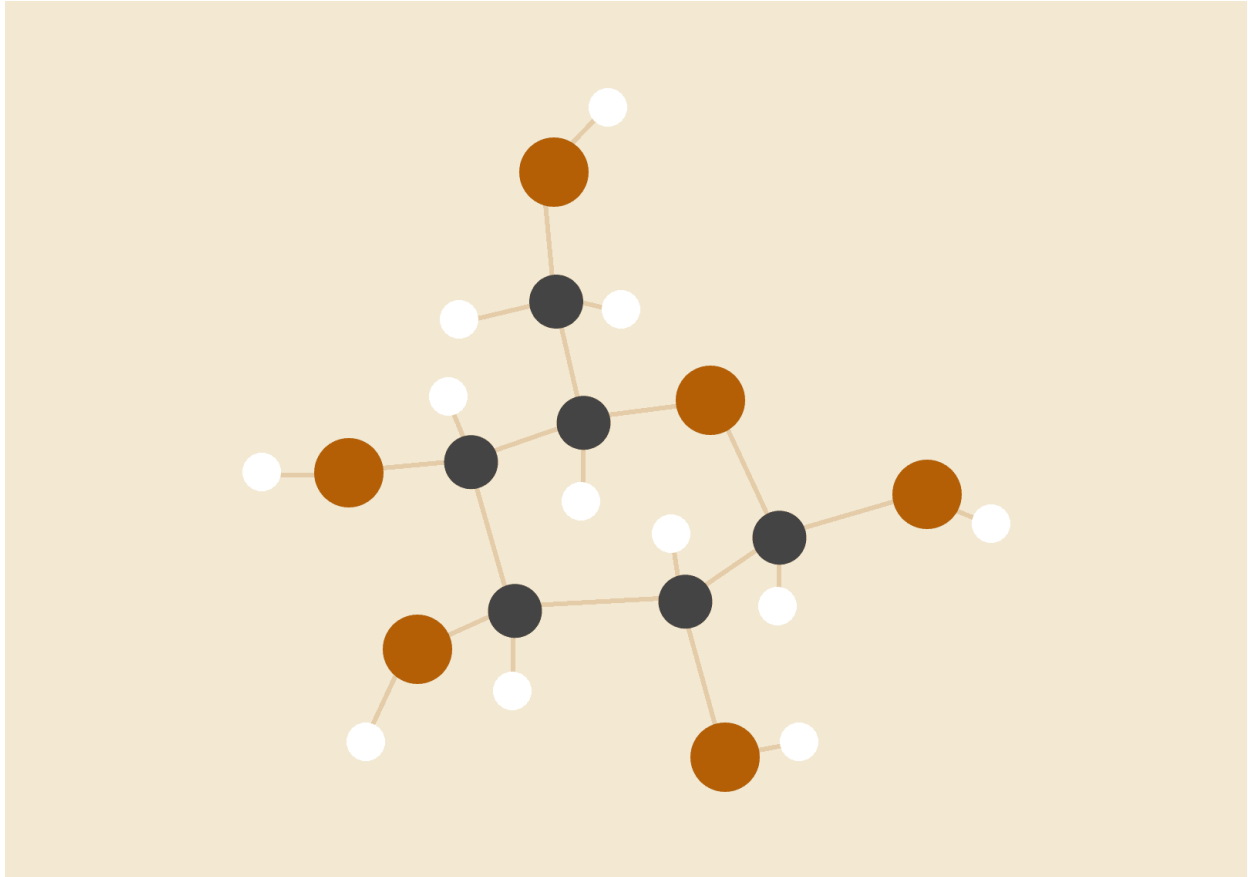


Algoridash User Guide



Muhammad Ennaayattulla

Admin No: 192026S

Module Group: 3

OVERVIEW

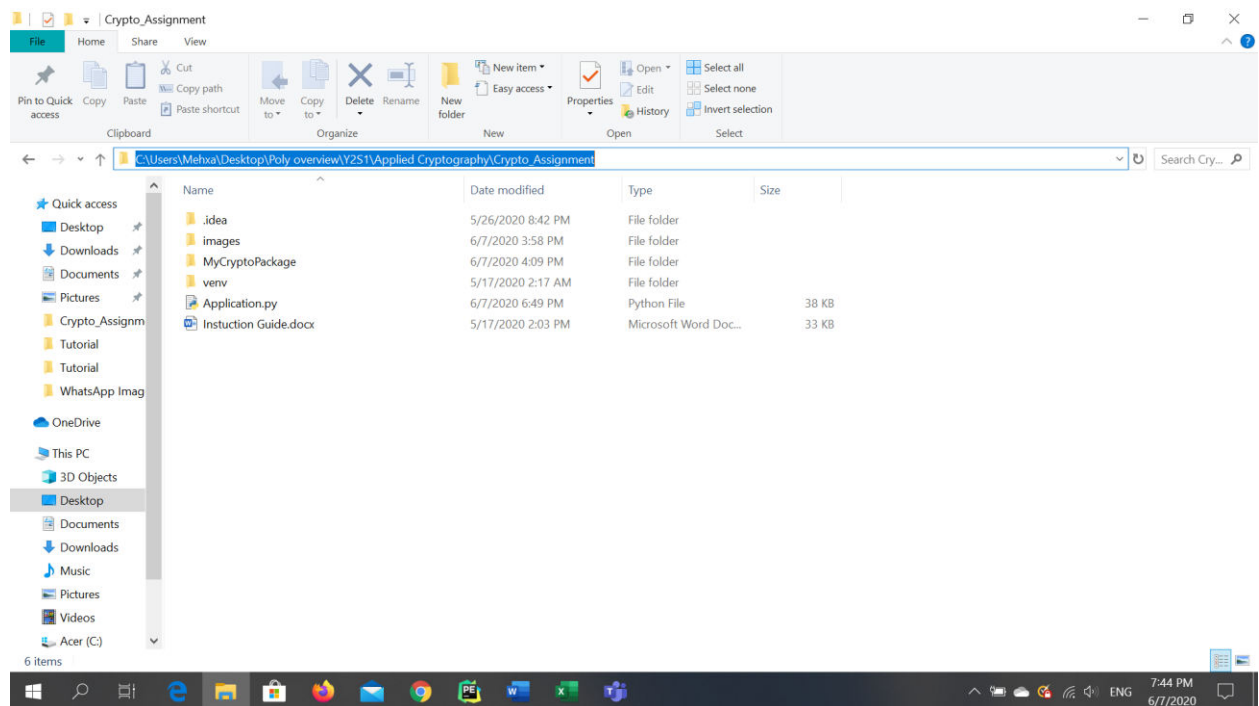
Algoridash is a simple encryption desktop application that also includes a mini lesson on Security Management Practices. This user guide will provide instructions on how to run the application as well as how to use the core functionalities in the application.

START

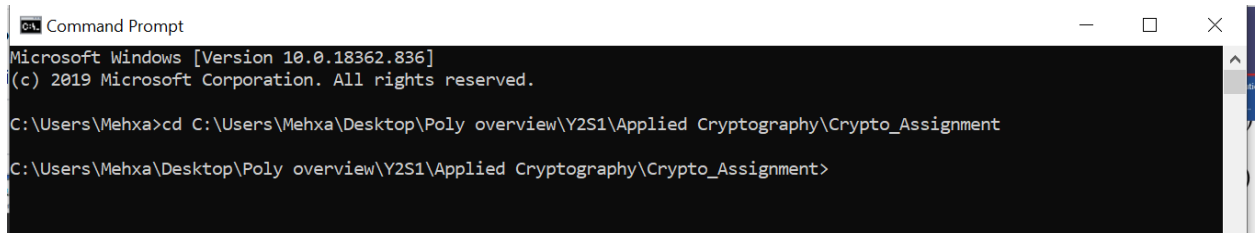
To run Algoridash, do the following steps:

1. Open command prompt
2. Use the change directory (cd) command to browse through your folders to find the downloaded application.

You may use the File Explorer to get the path of the application. Open File Explorer and navigate to the folder where you saved the application. Then copy the path from the breadcrumb.



Then paste the copied path into command prompt after typing “cd”

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.18362.836]", "(c) 2019 Microsoft Corporation. All rights reserved.", "C:\Users\Mehxa>cd C:\Users\Mehxa\Desktop\Poly overview\Y2S1\Applied Cryptography\Crypto_Assignment", and "C:\Users\Mehxa\Desktop\Poly overview\Y2S1\Applied Cryptography\Crypto_Assignment>". The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

```
Command Prompt
Microsoft Windows [Version 10.0.18362.836]
(c) 2019 Microsoft Corporation. All rights reserved.

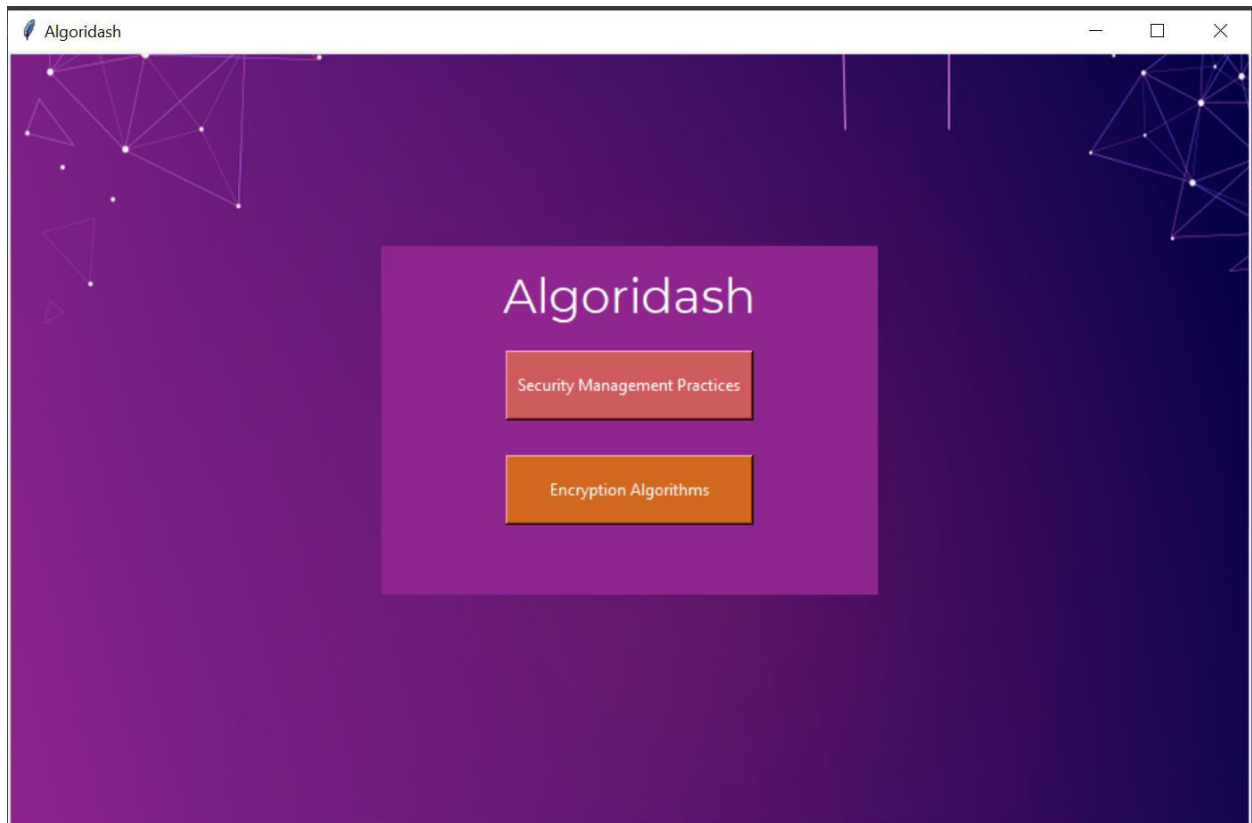
C:\Users\Mehxa>cd C:\Users\Mehxa\Desktop\Poly overview\Y2S1\Applied Cryptography\Crypto_Assignment

C:\Users\Mehxa\Desktop\Poly overview\Y2S1\Applied Cryptography\Crypto_Assignment>
```

Pressing enter will show that the path has been updated to the application folder.

3. Then, in command prompt, type **python Application.py** and run the code. The application should start up and show you the homepage.

HOMEPAGE



At the homepage you will notice two main buttons

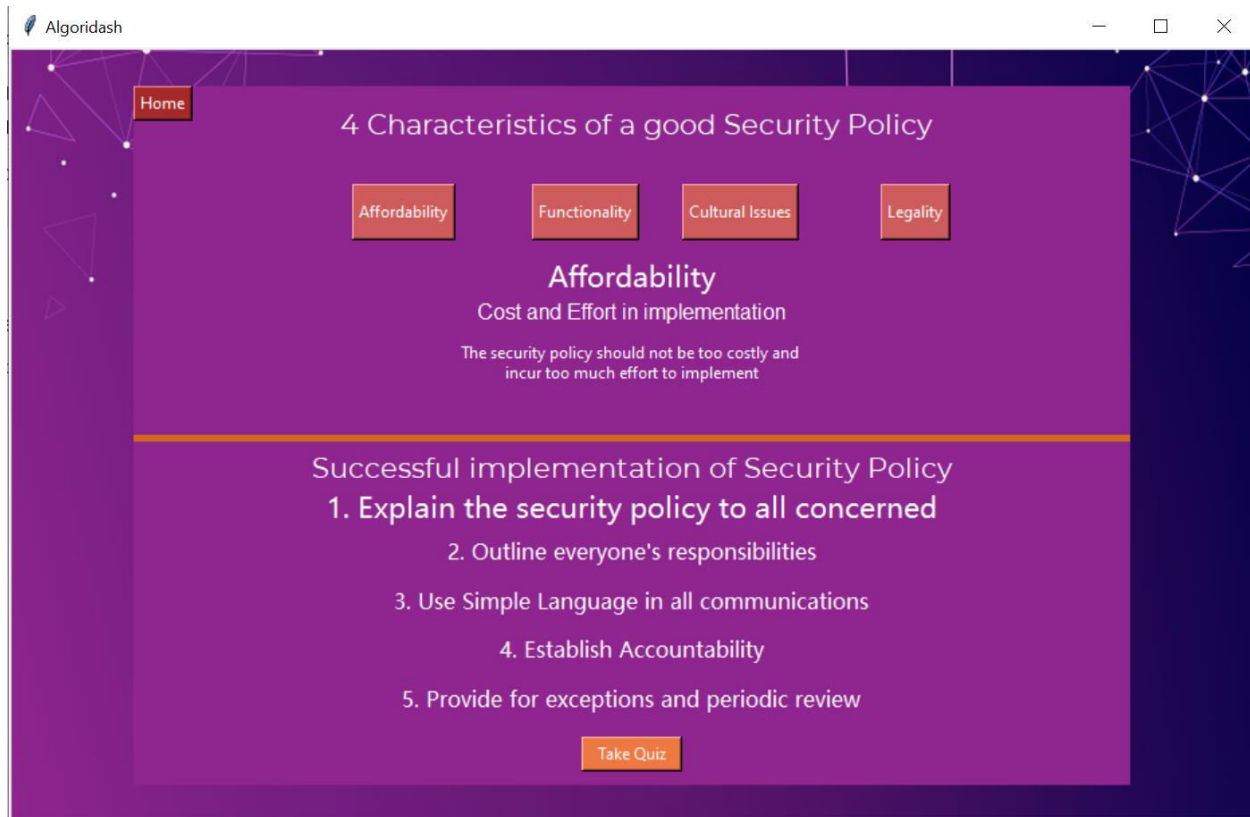
- 1. Lesson Button:**

This button will take you to the page in Algoridash with the lesson on Security Management Practices

- 2. Algorithms Button:**

This button will take you to the encryption algorithms page in Algoridash

LESSON



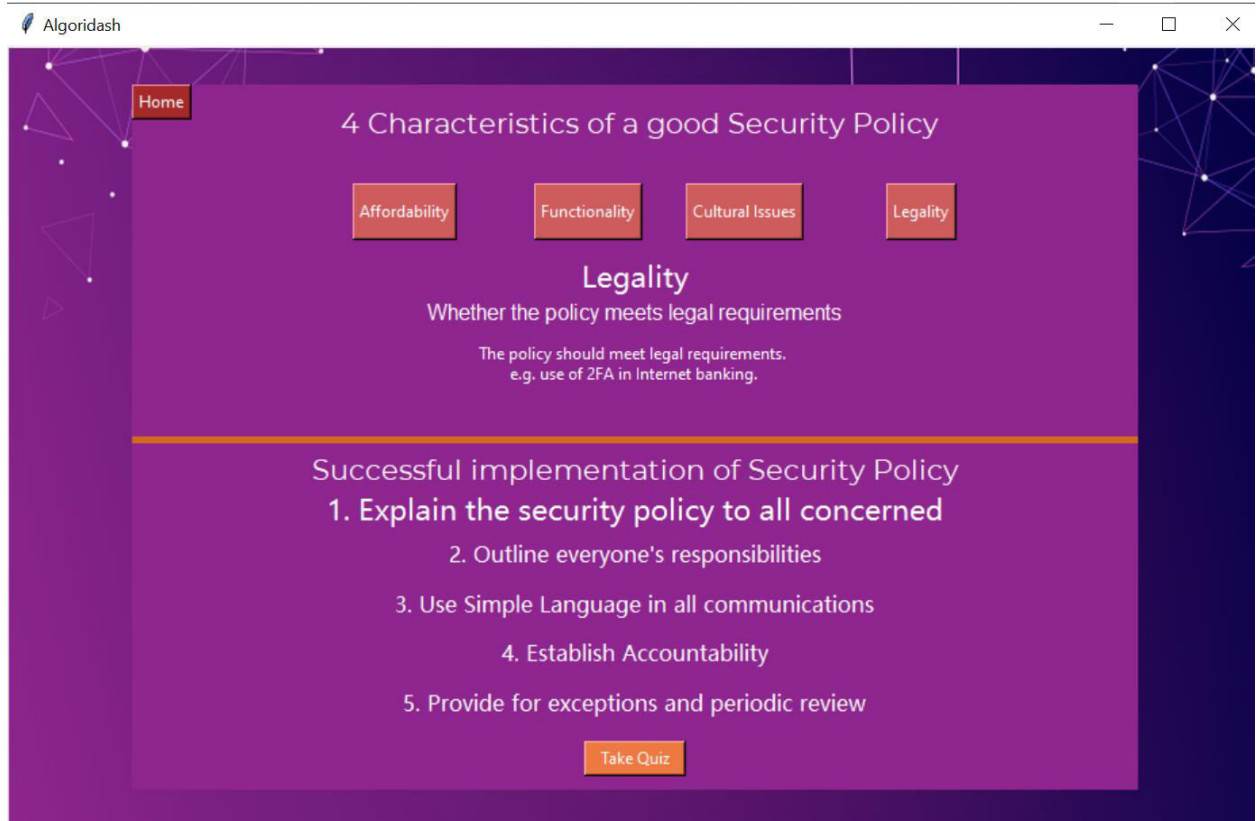
Clicking on the Security Management Practices button (**Lesson Button**) in the **homepage** or the **Back to Lesson button** in the **Results page**, will bring you to the **Lesson page**. The top section describes the 4 characteristics of a good security policy while the bottom section lists the criteria for successful implementation of Security Policy.

1. Home Button:

This button will return you to the homepage.

2. Characteristic Buttons:

Clicking on these buttons will change the characteristic being displayed and explained. For e.g if you were to click the Legality Button,

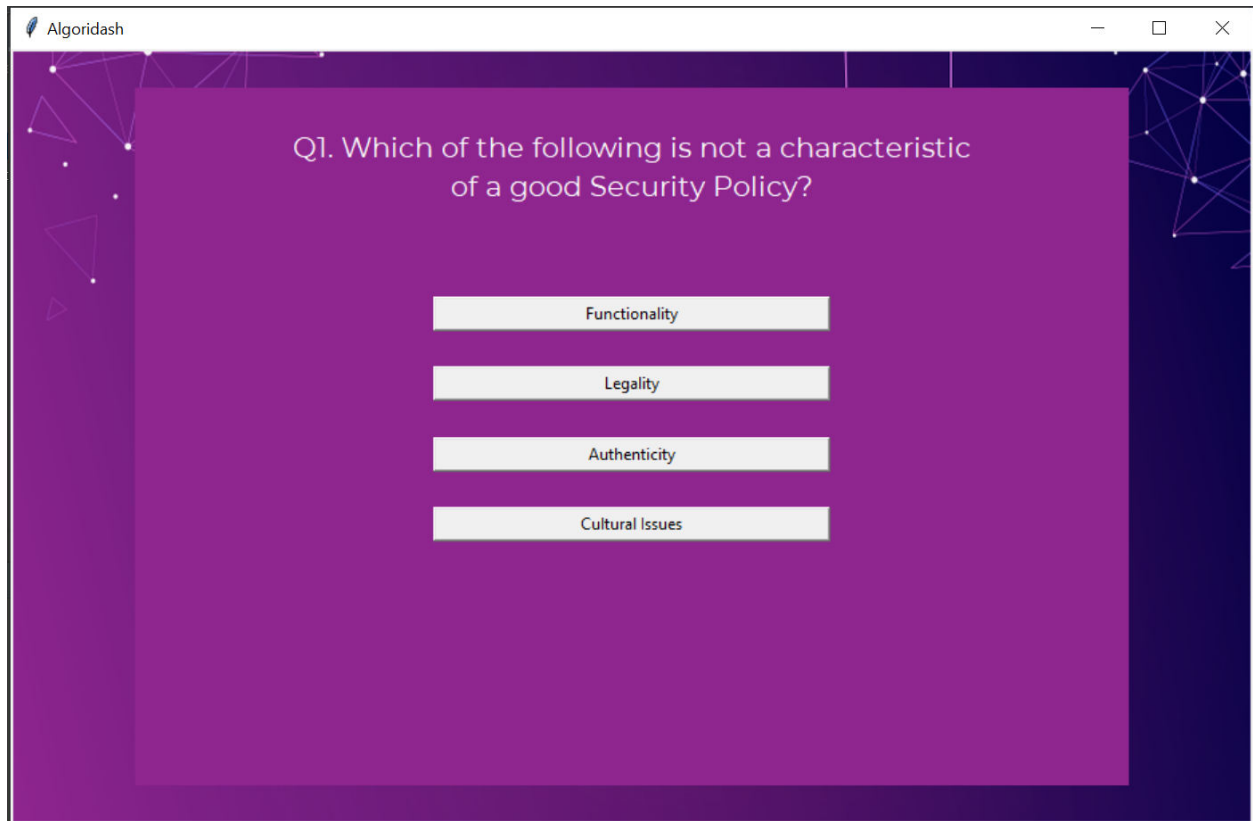


The layout changes to now explain legality as a characteristic.

3. Quiz Button

The quiz button will bring you to the quiz page and the quiz will automatically start. There is no time limit for the quiz. Once the quiz has begun, you will be unable to leave the quiz page until you have answered the quiz questions.

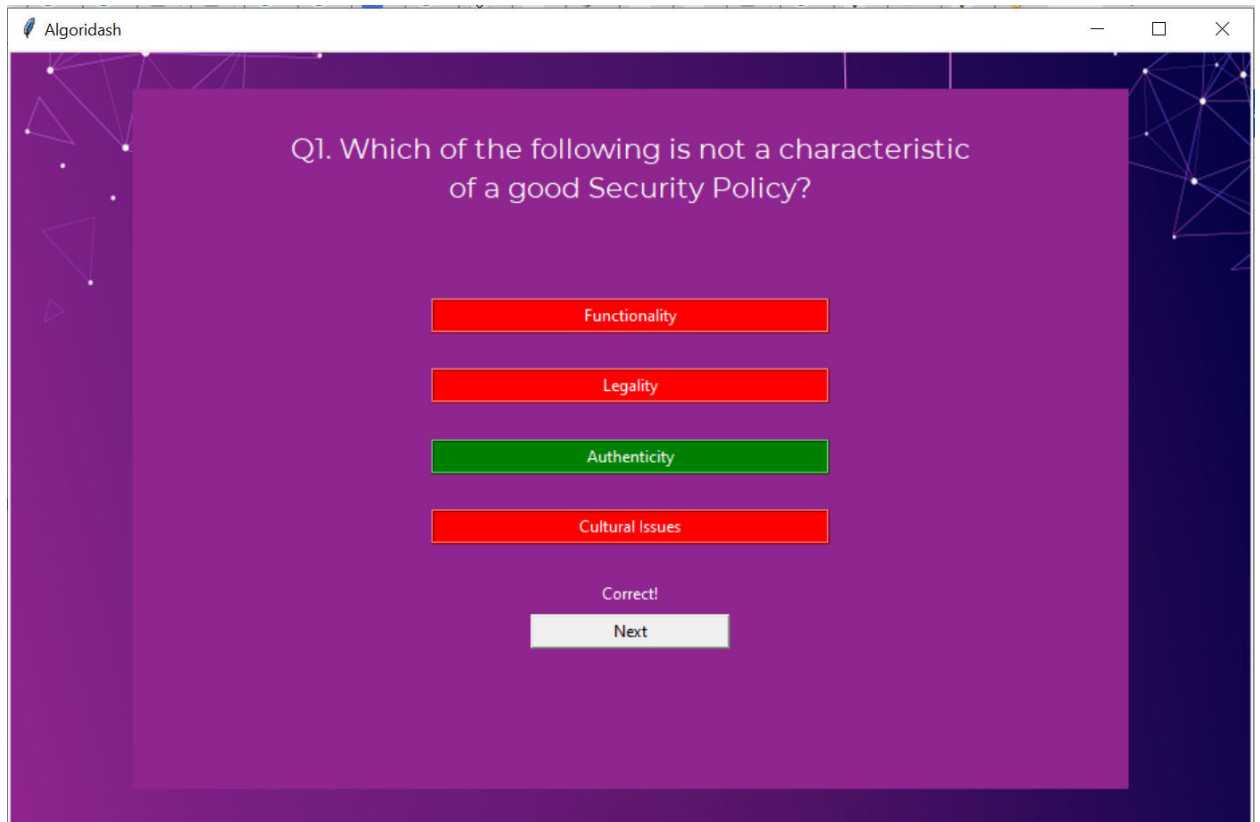
QUIZ



Clicking on the **Quiz button** on the **Lesson Page** will bring you to the **Quiz page**. Each question is a multiple choice question with 4 answers. The scores will be added and revealed to you once the quiz is over.

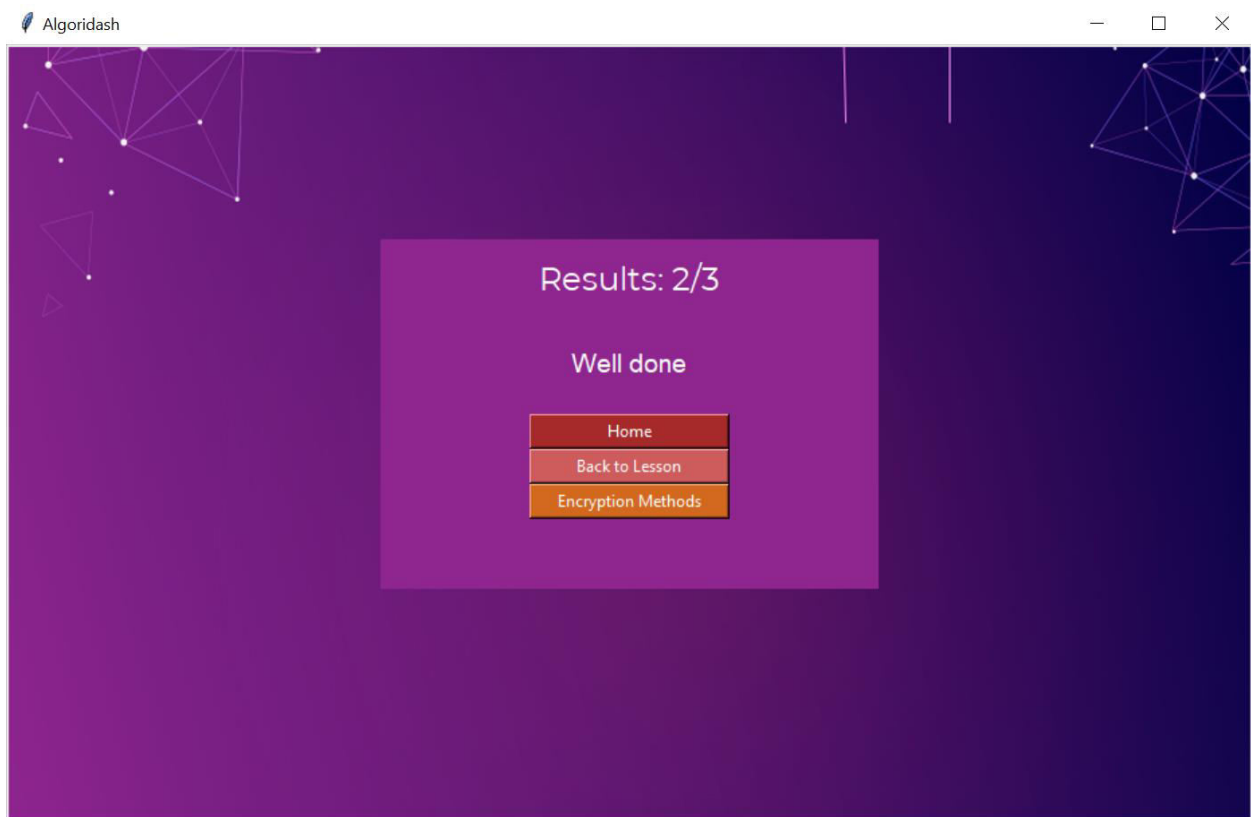
1. Option Buttons

The option buttons represent the possible answers to the question. Clicking on one of the option buttons will reveal the correct answer.



However, choose wisely as once clicked, you may not change your answer. After you have clicked an option, the next button will appear to bring you to the next question. After the last question, the next button becomes the **View Results Button**

RESULTS



Clicking on the **View Results Button** on the last question page will reveal your final results and three buttons.

- 1. Home Button:**

This button returns you to the home page.

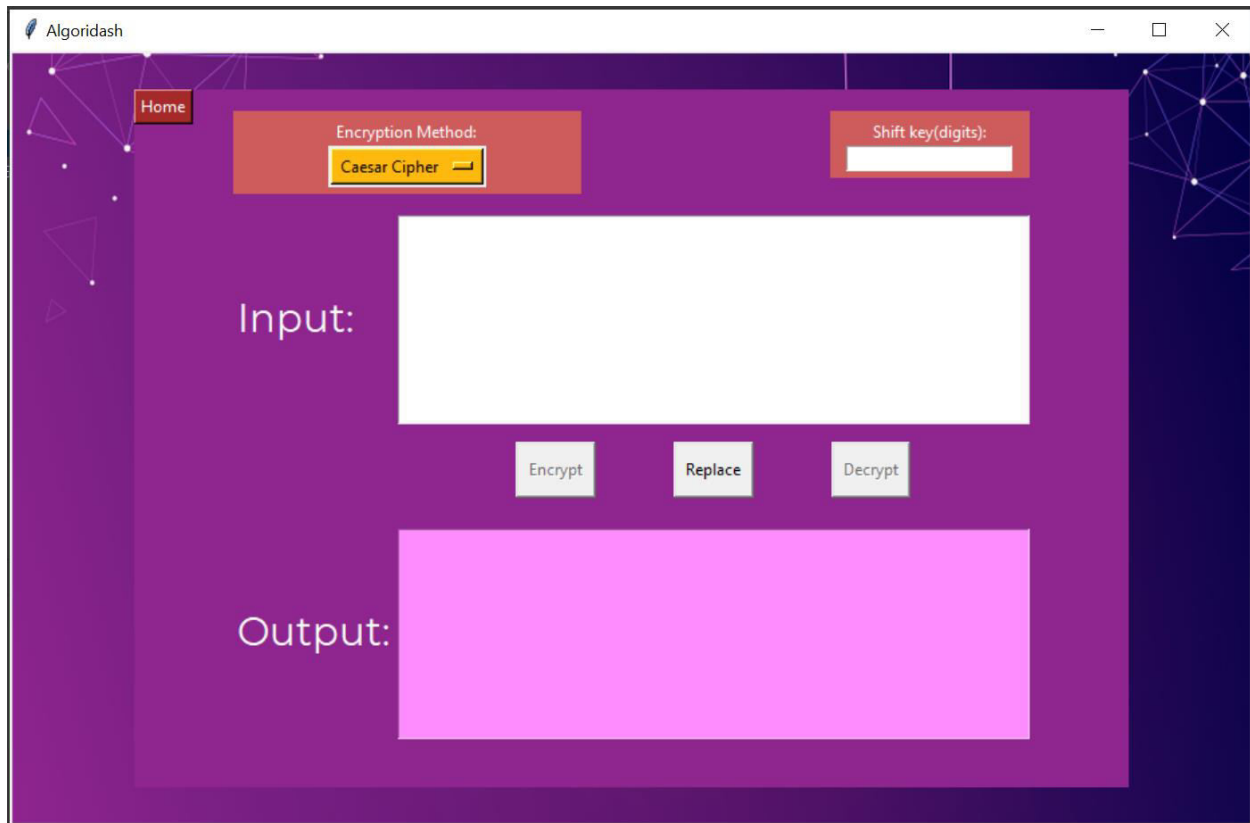
- 2. Back to Lesson Button:**

This button returns you back to the Lesson page.

- 3. Encryption Methods Button:**

This button brings you to the encryption algorithms page in Algoridash.

ENCRYPTION



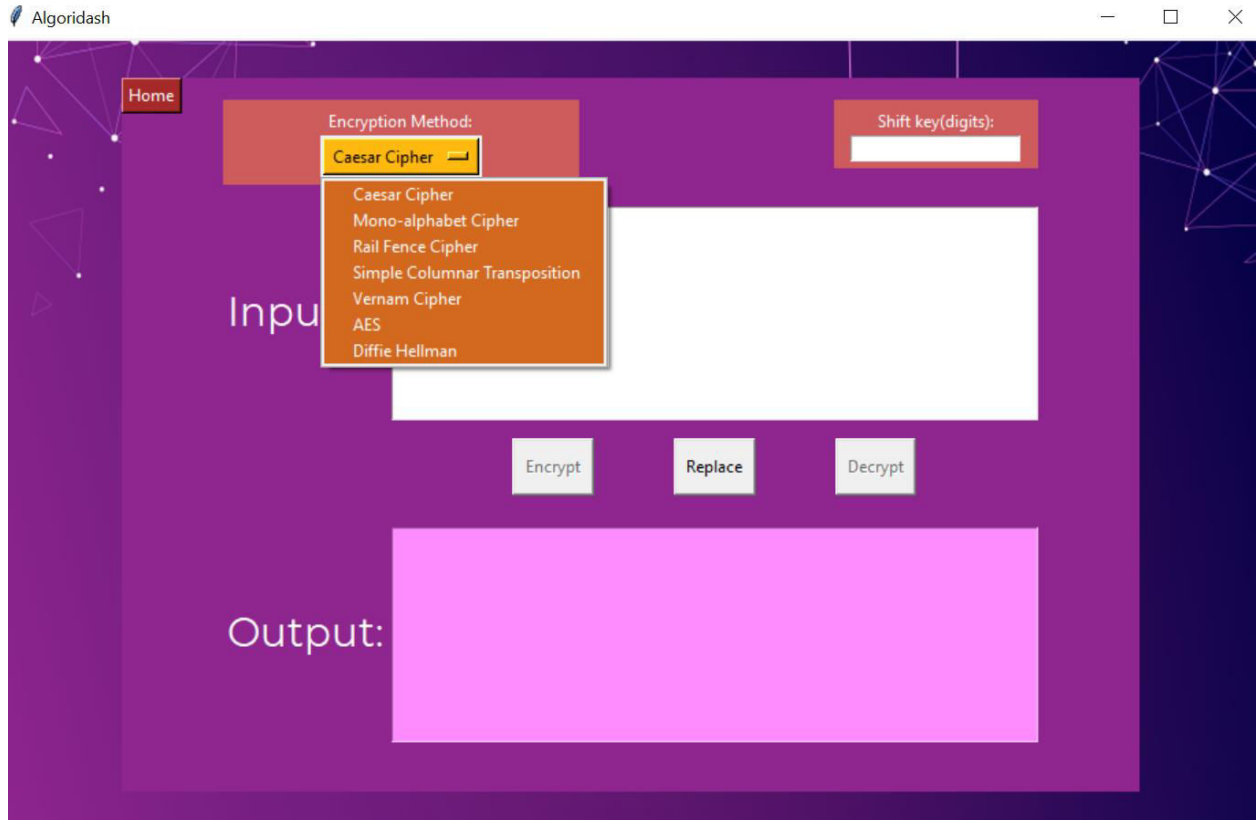
Clicking on the **Encryption Methods Button** at either the **homepage** or the **View Results page** will bring you to the **Encryption page**. Here, you can choose from 7 different encryption methods[**Caesar Cipher**, **Railfence Cipher**, **Simple Columnar Transposition**, **Mono-alphabet Cipher**, **Vernam Cipher**, **AES**, **Diffie Hellman Key Exchange**] to encrypt or decrypt secret messages. The default method is **Caesar Cipher**. This is the main layout for most of the algorithms. However for **Vernam Cipher**, **AES** and **Diffie Hellman Key Exchange**, the layout would be different.

1. Home Button:

This button returns you to the homepage

2. Encryption Method:

Clicking on this button will show an OptionMenu (dropdown) of all the available encryption methods.



Choosing a different method will change the **Special value** required for the encryption methods and even the layout for **Vernam Cipher**, **AES** and **Diffie Hellman Key Exchange**

3. Shift Key(Special):

This is the input for the **special value** needed for each encryption method. For **Caesar Cipher**, it is **Shift Key**. If you select **Railfence Cipher** from the **Encryption Method OptionMenu**, it will change to **Rows**. Similarly for **Mono-alphabet cipher** and **Simple Columnar Transposition** it will change to **Key**. Please **DO NOT** key in **non-numeric** inputs for **Caesar Cipher** and **Railfence Cipher**. Also **ENSURE** that your key for **Mono-alphabet Cipher** is the **26 alphabets** but rearranged. **Failure** to do so will result in an **error** causing **incorrect output** or **no output**.

4. Input Box:

The input box is where you can enter your plaintext. After entering the **Special Value** and pressing the **Encrypt Button**, the ciphertext will appear at the **Output Box**.

5. Encrypt Button:

The **Encrypt Button** is disabled by default and will only be normal after both **Special Value** and **Input Box** have values in them. Clicking on this button will encrypt the plaintext in the **Input Box** and return the encrypted value in the **Output Box**

6. **Replace Button:**

This button places the output from the **Output Box** into the **Input Box**. This will allow you to decrypt the ciphertext to retrieve the plaintext you just encrypted

7. **Decrypt Button:**

The **Decrypt Button** is disabled by default and will only be normal after both **Special Value** and **Input Box** have values in them. Clicking on this button will decrypt the ciphertext in the **Input Box** and return the plaintext value in the **Output Box**

AES LAYOUT

The screenshot shows a web application window titled "Algoridash". The interface has a dark purple background with a geometric pattern. A "Home" button is in the top left. The main area contains several input fields and buttons. At the top, there are three dropdown menus: "Encryption Method:" with "AES" selected, "Key Size(bits):" with "128" selected, and "Method:" with "CBC" selected. Below these are two input fields: "IV:" and "Key:", each with a "Generate" button to its right. In the center, there is a large white text input field labeled "Input:". Below the input field are three buttons: "Encrypt", "Replace", and "Decrypt". At the bottom, there is a large pink text area labeled "Output:". The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

Choosing the **AES** encryption method will return this layout. The difference between this layout and the normal layout is

- 1. Key Size(bits):**

This is a dropdown menu to select the key sizes, 128, 192 or 256 bits for encryption or decryption

- 2. Method:**

This is a dropdown menu to select the method of AES encryption, CBC, CFB, OFB and ECB.

- 3. IV:**

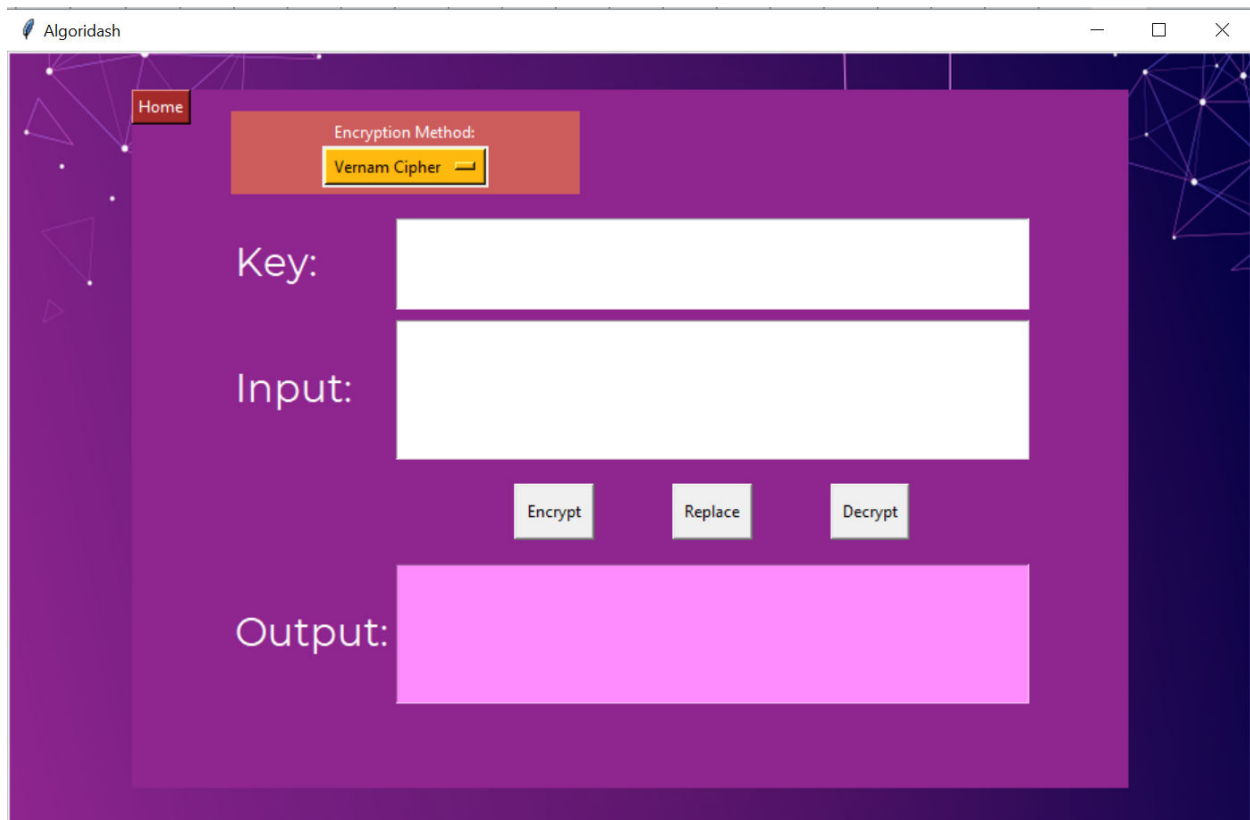
This entry is to input the IV for encryption/decryption. If you do not have an IV, you may generate one using the generate button

- 4. Key:**

This entry is to input the Key for encryption/decryption. If you do not have a Key, you

may generate one using the generate button.

VERNAM LAYOUT

The image shows a web application window titled "Algoridash". The interface has a dark purple background with a geometric pattern of white dots and lines. A central light purple rectangular area contains the main controls. At the top left of this area is a "Home" button. To its right is an "Encryption Method:" label above a dropdown menu currently showing "Vernam Cipher". Below these are two large white text input fields labeled "Key:" and "Input:". Under the input fields are three buttons: "Encrypt", "Replace", and "Decrypt". At the bottom is a large pink rectangular area labeled "Output:". The window has standard OS window controls (minimize, maximize, close) in the top right corner.

Choosing the **Vernam Cipher** encryption method will return this layout. The difference between this layout and the normal layout is

1. **Key:**

This entry is to input the key for encryption/decryption. Please **ENSURE** that the key is the SAME size as the input. **Failure** to do so will result in an **error** causing **incorrect output** or **no output**.

DIFFIE HELLMAN LAYOUT

The screenshot shows a web application window titled "Algoridash". Inside the window, there is a "Home" button in the top left corner. Below it, there is a section titled "Encryption Method:" with a dropdown menu showing "Diffie Hellman". Below this, there are four input fields labeled "Prime Number 1:", "Prime Number 2:", "Secret Number 1:", and "Secret Number 2:". At the bottom of this section is a button labeled "Get Key". The background of the application is a dark purple color with a geometric pattern of white dots and lines.

Choosing the **Diffie Hellman Key Exchange** method will return this layout. The difference between this layout and the normal layout is

1. **Prime Numbers 1 & 2:**

These entries are to input the numbers decided by both parties. Please **ENSURE** that the numbers are **PRIME NUMBERS**. **Failure** to do so will result in an **error** causing **incorrect output** or **no output**.

2. **Secret Numbers 1 & 2:**

These entries are to input the numbers decided chosen privately by both parties

3. **Get Key Button:**

Clicking on this button reveals the key used that is exchanged by both parties.