**D’ Crypt User Guide**

*by Ko Jia Ling*

**Introduction**

D' Crypt is a web-based Python application that aims to enhance the learning of selected cryptography topics. It provides cryptography tools for encryption and decryption, as well as explanations on cryptography theory.

# Table of Content

[Table of Content 1](#_Toc42212089)

[Starting the Application 2](#_Toc42212090)

[Home Page/Menu 3](#_Toc42212091)

[Tools – Default Format 4](#_Toc42212092)

[Tools – AES 5](#_Toc42212093)

[Tools – Mono-alphabet Cipher 6](#_Toc42212094)

[Tools – Rail Fence Technique 7](#_Toc42212095)

[Tools – Shift Cipher 8](#_Toc42212096)

[Tools – Simple Columnar Transposition Technique 9](#_Toc42212097)

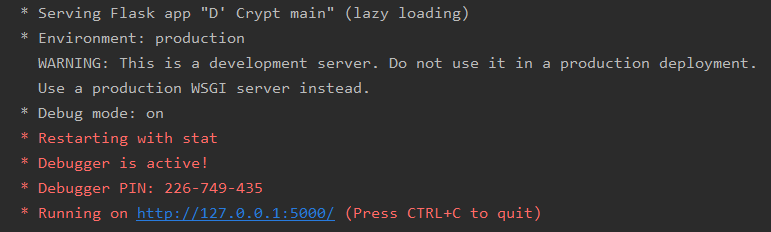
[Tools – Vernam Cipher 10](#_Toc42212098)

[Tools – Diffie-Hellman Key Exchange 11](#_Toc42212099)

[Learn 12](#_Toc42212100)

# Starting the Application

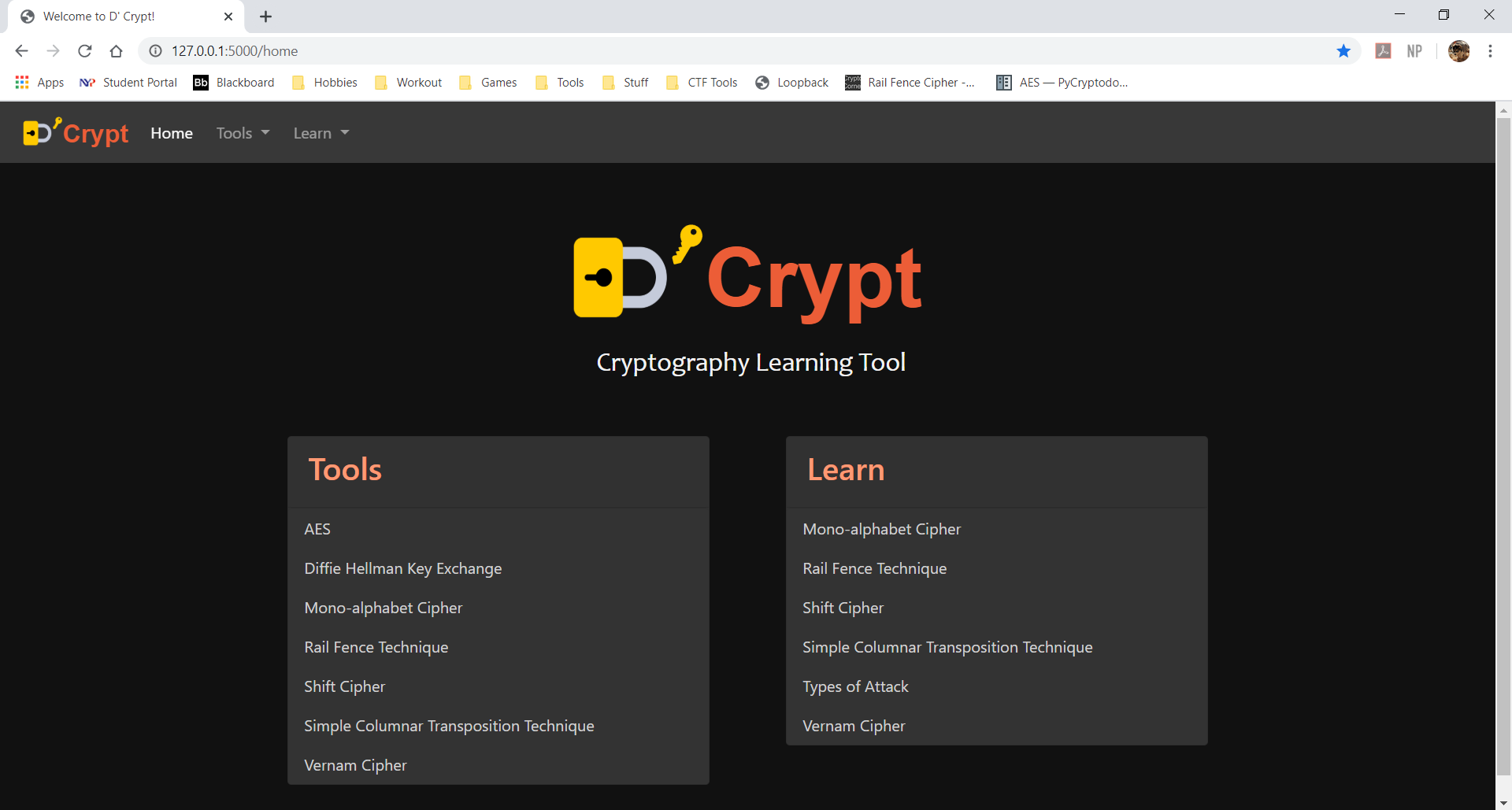
1. Run D’ Crypt main.py, you should see the following message in the console.



1. Open a browser and visit <http://127.0.0.1:5000/>

# Home Page/Menu

Route: <http://127.0.0.1:5000/home>



The home page/menu is the landing page upon accessing application.

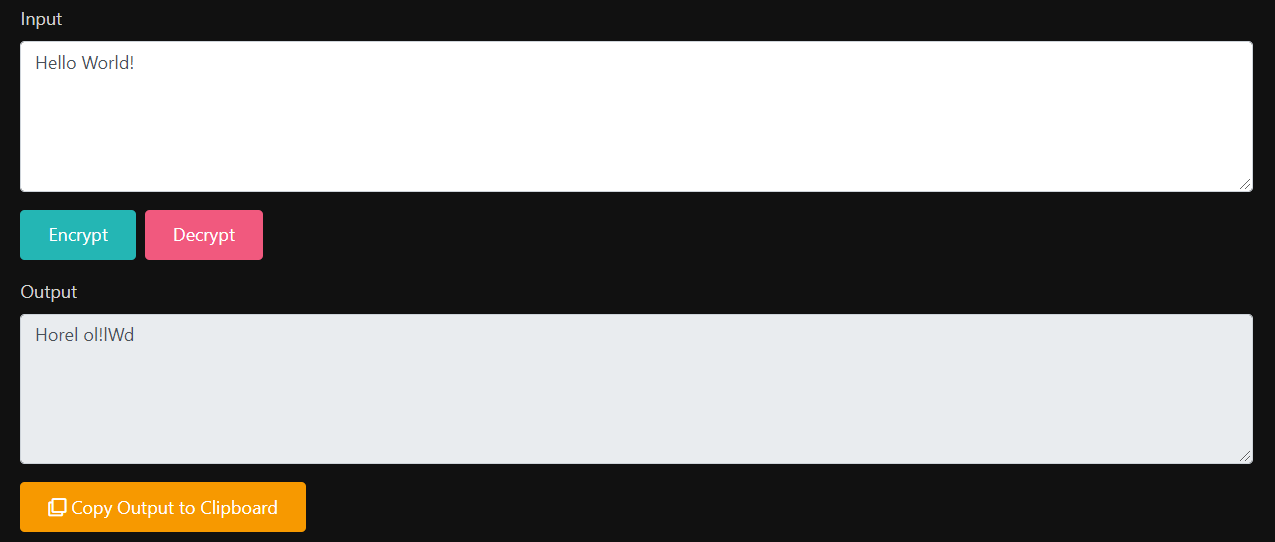
The page contains a navigation pane for all Tools and Learning materials.

# Tools – Default Format

Route: http://127.0.0.1:5000/learn/[tool name]

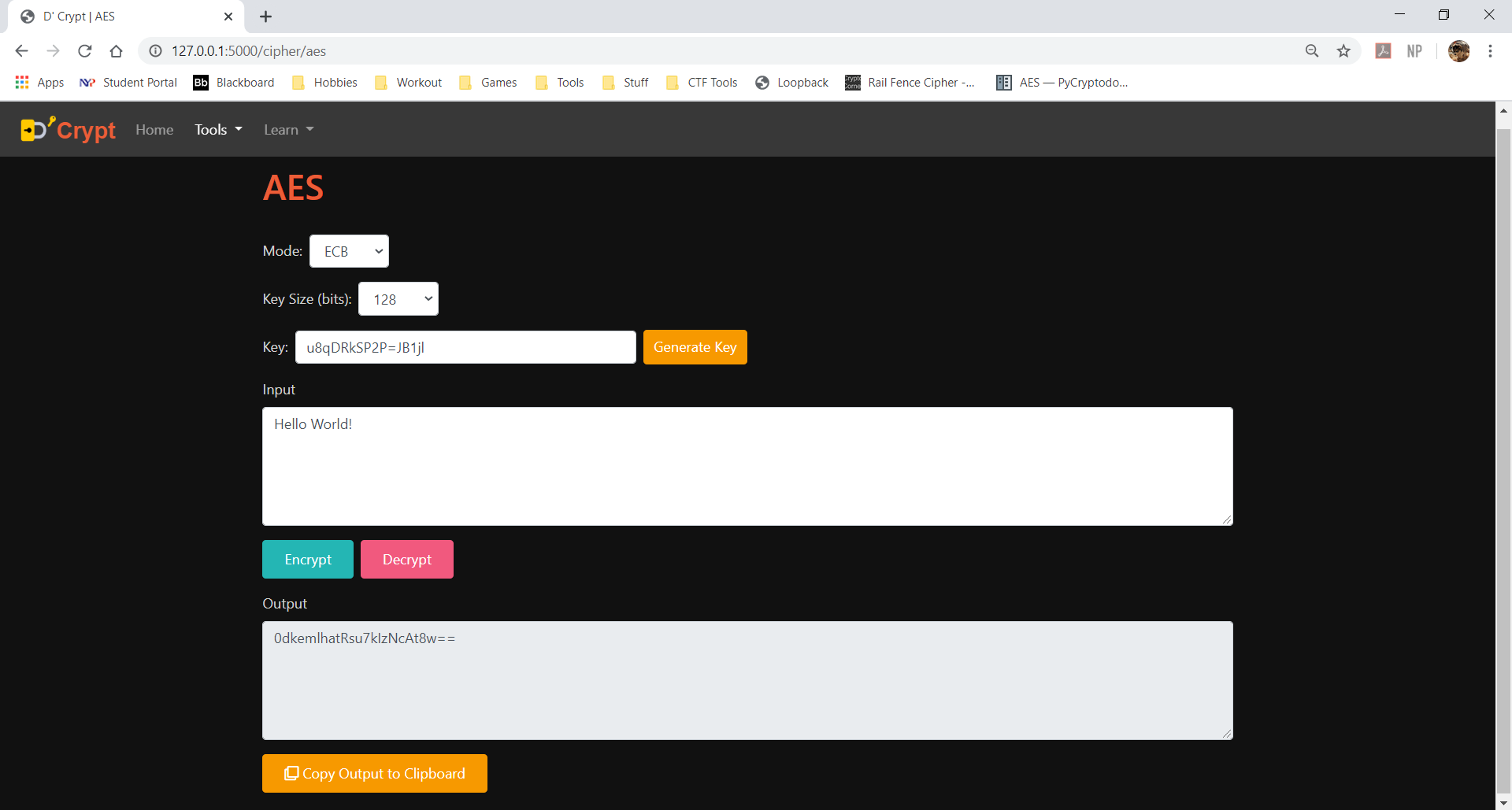
Most of the tools (except Diffie-Hellman Key Exchange) will have an Input and Output box. How it works is as follows:

1. Enter the plaintext/ciphertext into the Input box.
2. Click either the Encrypt or Decrypt button.
3. The generated plaintext/ciphertext will appear in the Output box.
4. Click on the Copy Output to Clipboard button to copy the output.



# Tools – AES

Route: <http://127.0.0.1:5000/cipher/aes>



Function: Encrypts/Decrypts text using AES.

4 modes available:

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

3 Key sizes:

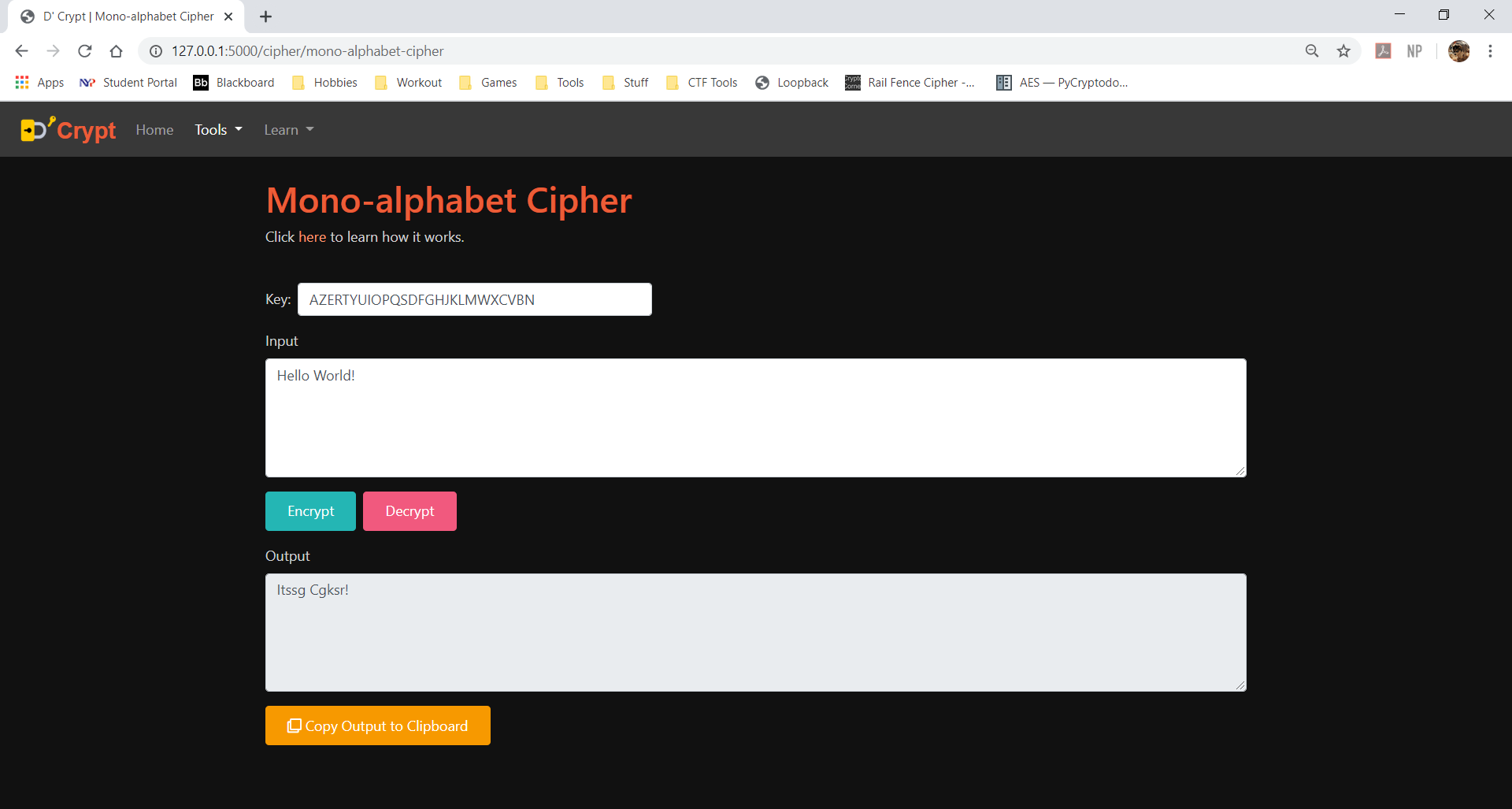
1. 128 bits (16 bytes)
2. 192 bits (24 bytes)
3. 256 bits (32 bytes)

Initialization Vector (IV) size: 128 bits

IV is only applicable for CBC, CFB and OFB mode.

# Tools – Mono-alphabet Cipher

Route: <http://127.0.0.1:5000/cipher/mono-alphabet-cipher>



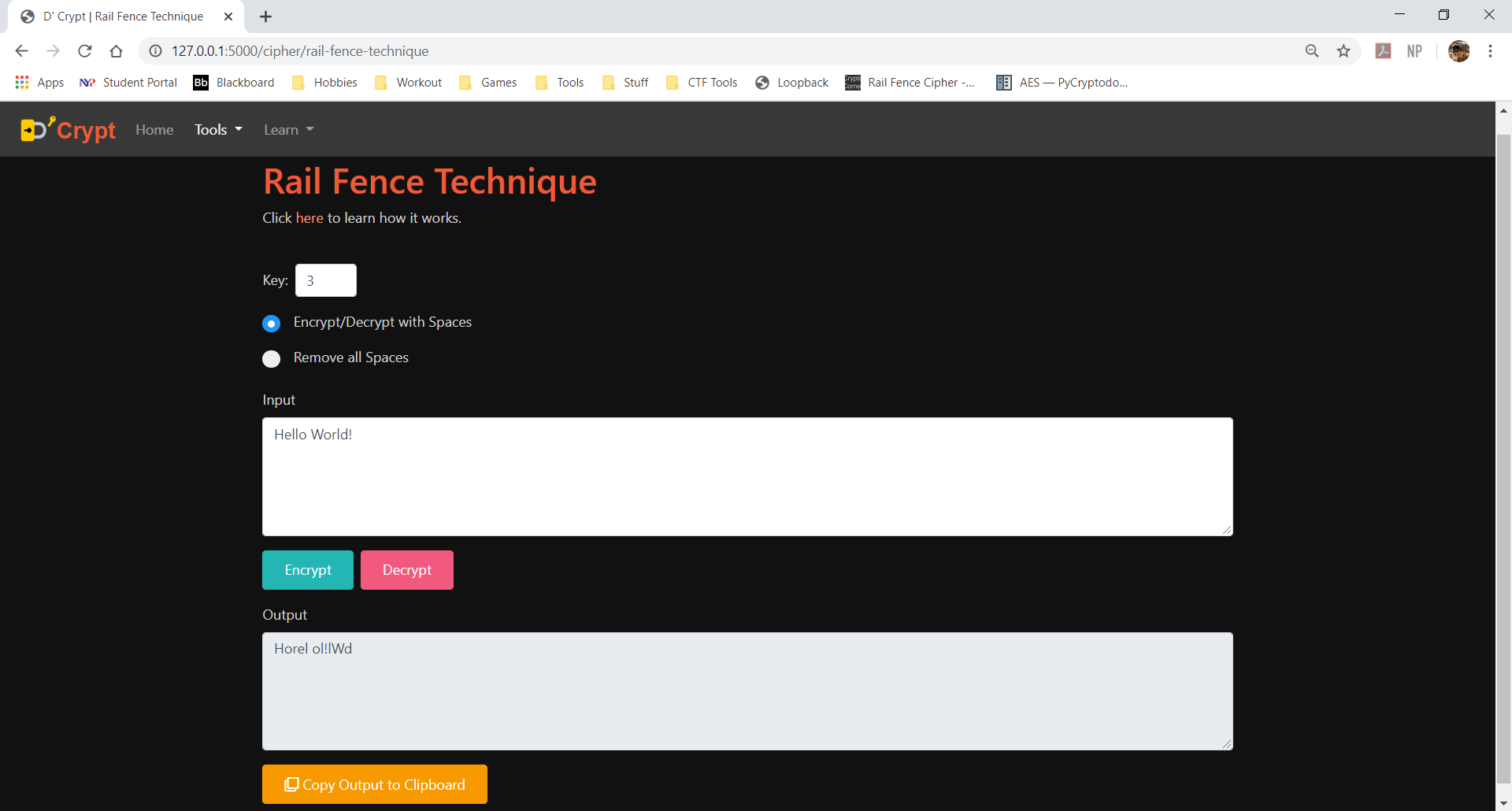
Function: Encrypts/Decrypts text using Mono-alphabet Cipher. Note that this tool does not encrypt/decrypt special characters and spaces.

Conditions for Key:

* Key must contain all 26 letters of the alphabet.
* Key should not have repeating letters. (i.e. there should not be more than one ‘A’, ‘B’ etc.)

# Tools – Rail Fence Technique

Route: <http://127.0.0.1:5000/cipher/rail-fence-technique>



Function: Encrypts/Decrypts text using Rail Fence Technique.

Conditions for Key:

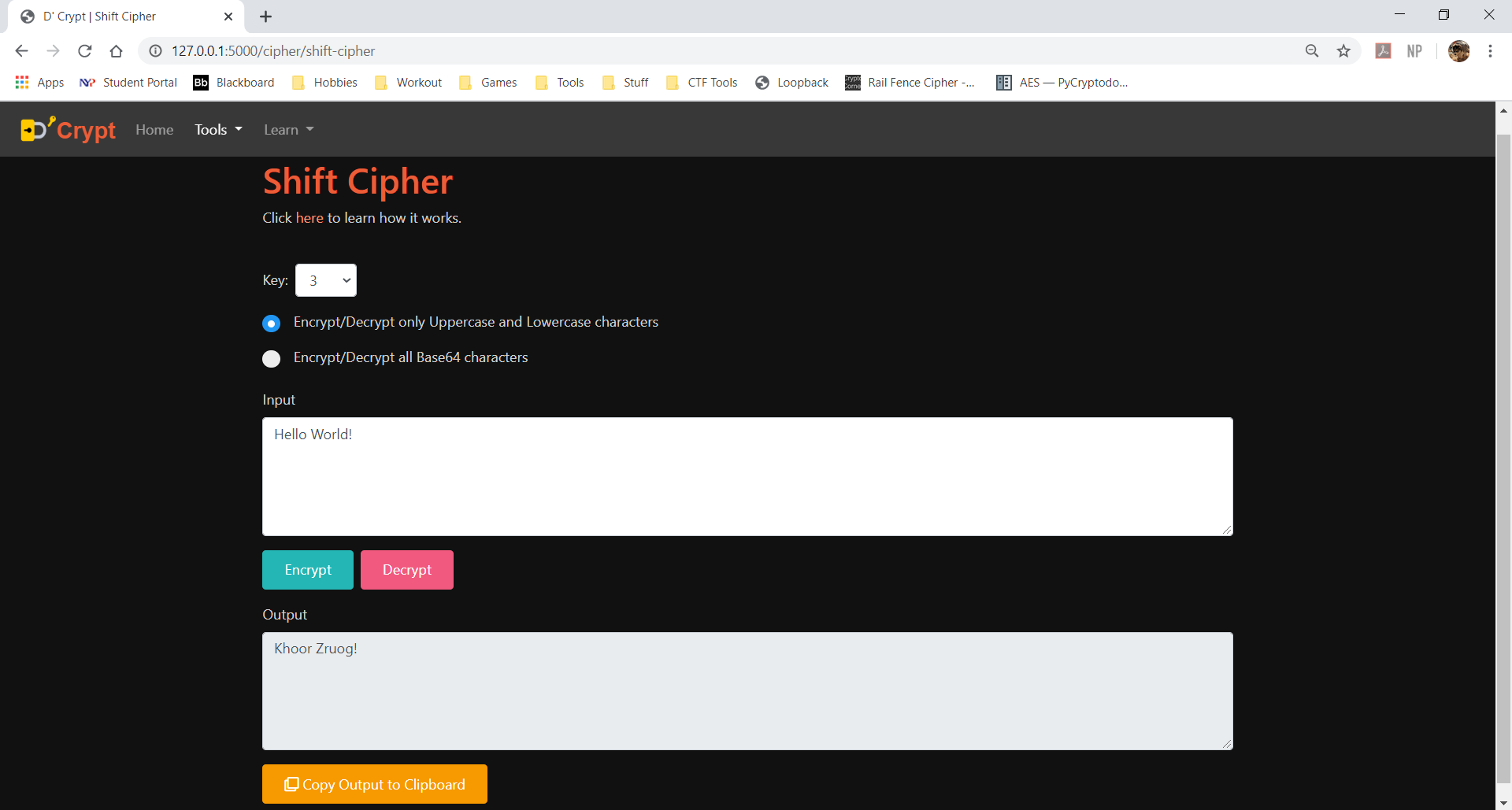
* Minimum value of 2.
* Maximum value of 1000.

2 modes:

1. Encrypt/Decrypt with Space
2. Remove all Spaces

# Tools – Shift Cipher

Route: <http://127.0.0.1:5000/cipher/shift-cipher>



Function: Encrypts/Decrypts text using Shift Cipher.

Conditions for Key:

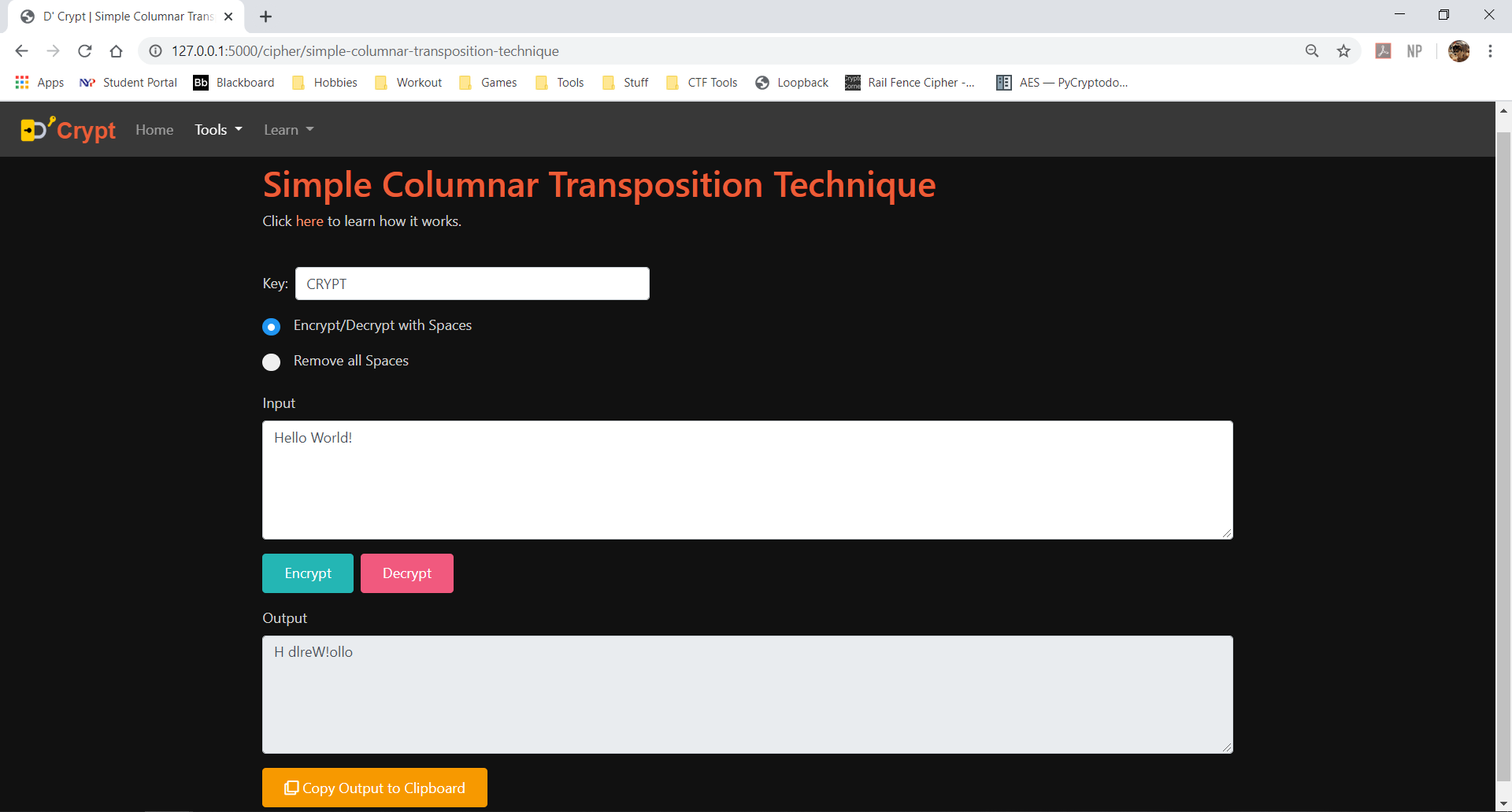
* Minimum value of 1.
* Maximum value of 26.

2 modes:

1. Encrypt/Decrypt only Uppercase and Lowercase characters (i.e. only alphabets)
2. Encrypt/Decrypt all Base64 characters.

# Tools – Simple Columnar Transposition Technique

Route: <http://127.0.0.1:5000/cipher/simple-columnar-transposition-technique>



Function: Encrypts/Decrypts text using Simple Columnar Transposition Technique.

Conditions for Key:

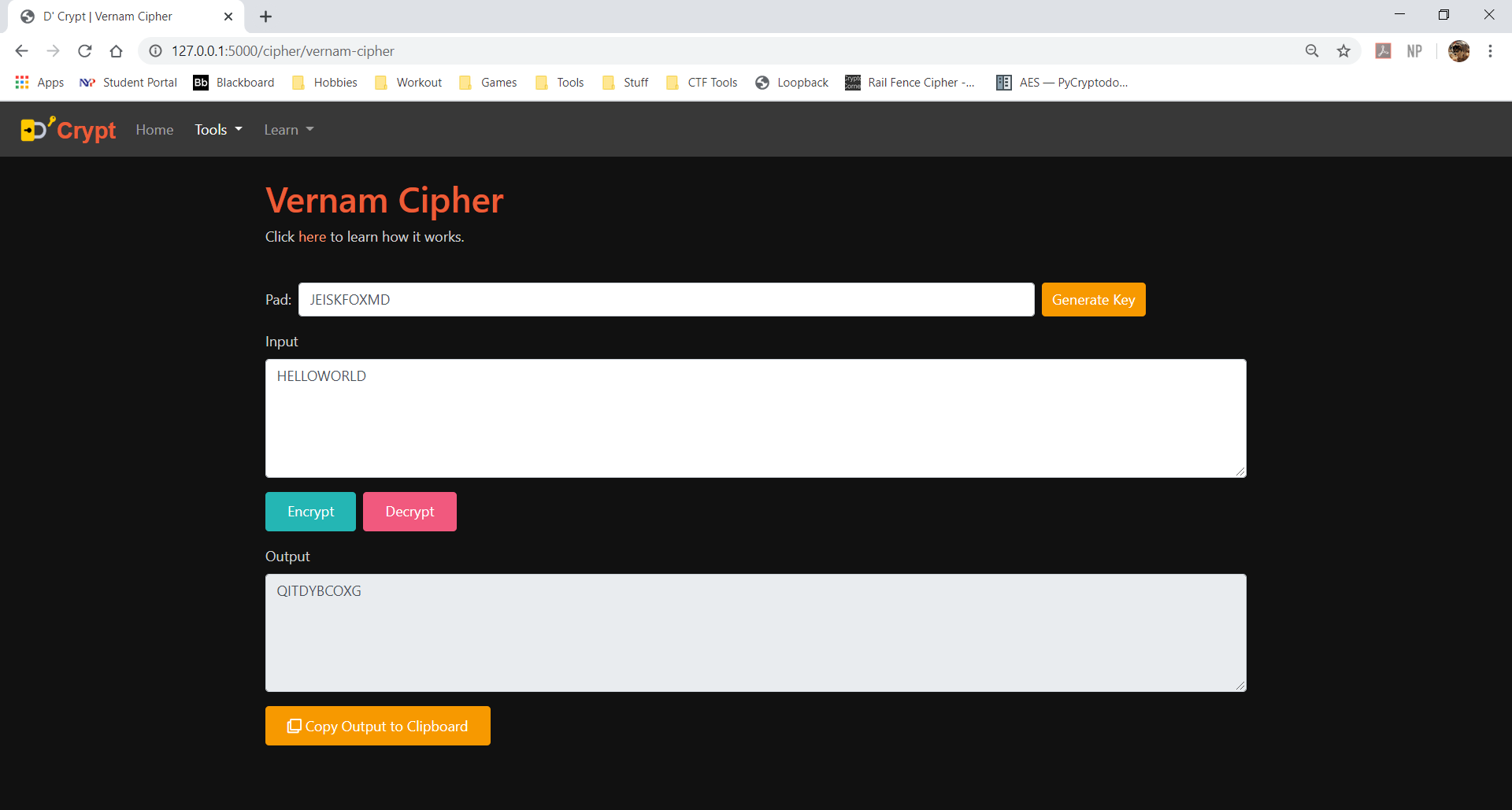
* Only accepts alphanumeric values. (i.e. A-Z, a-z, 0-9)

2 modes:

1. Encrypt/Decrypt with Space
2. Remove all Spaces

# Tools – Vernam Cipher

Route: <http://127.0.0.1:5000/cipher/vernam-cipher>



Function: Encrypts/Decrypts text using Vernam Cipher.

Conditions for Pad:

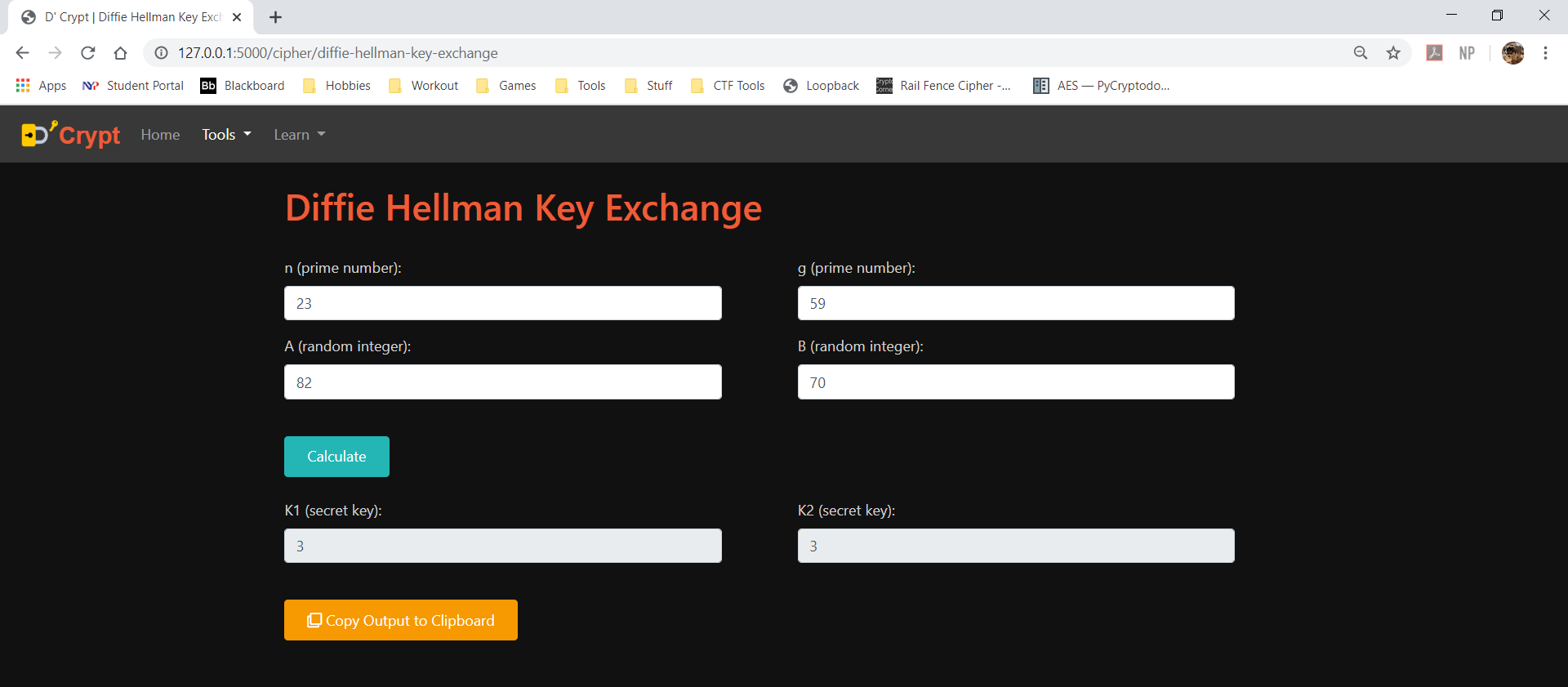
* Must be of equal length as input text.
* Only contain alphabets (uppercase and lowercase letters).

Conditions for Input:

* Must be of equal length as pad.
* Only contain alphabets (uppercase and lowercase letters).

# Tools – Diffie-Hellman Key Exchange

Route: <http://127.0.0.1:5000/cipher/diffie-hellman-key-exchange>



Function: Calculate key based on Diffie-Hellman Key Exchange.

Conditions for n and g:

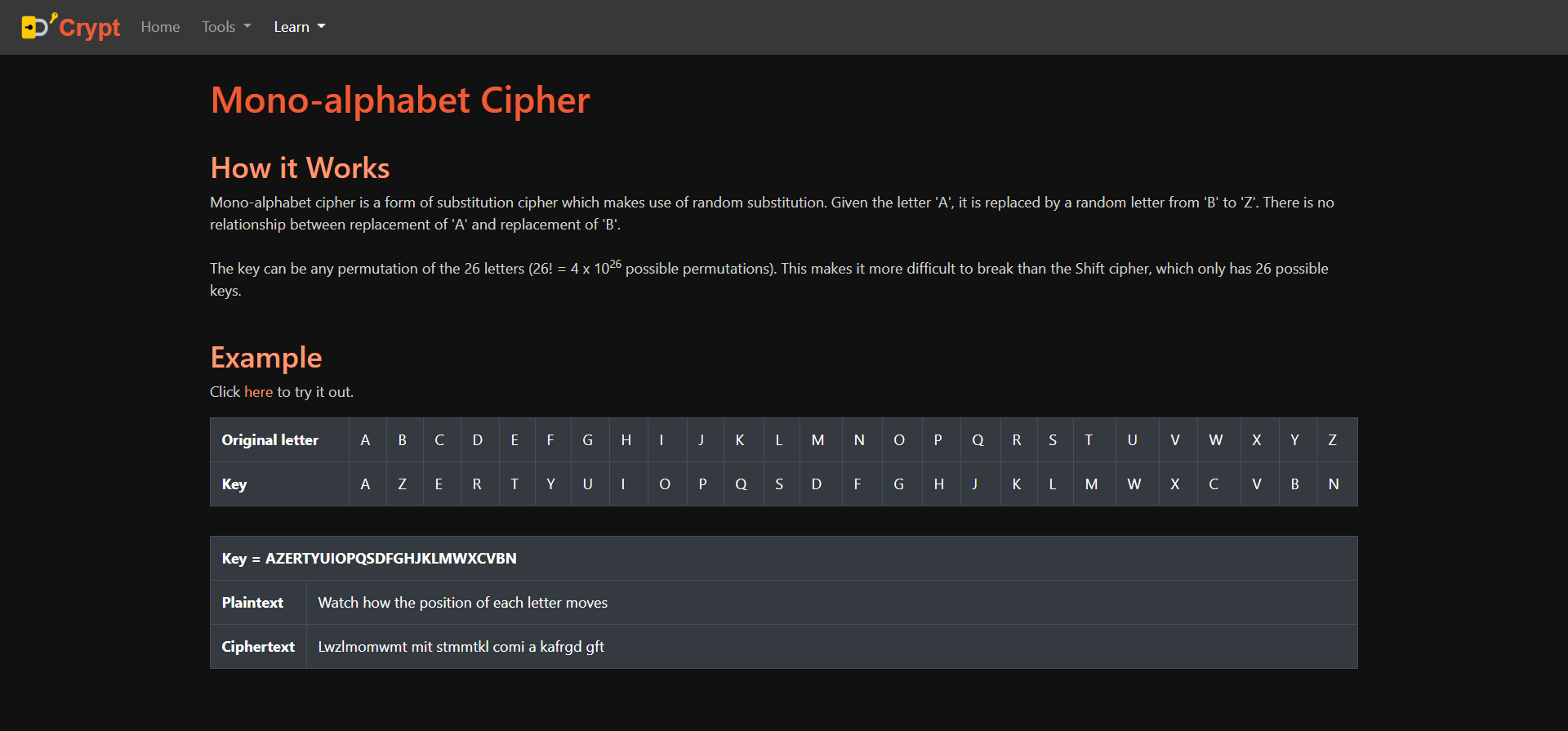
* Must be prime numbers.

Conditions for A and B:

* Must be whole numbers (0 and above).

# Learn

Route: http://127.0.0.1:5000/learn/[topic]



Pages under the “Learn” section provides explanations about various cryptography topics.