Test Cases:

# Caesar Cipher:

## Encryption:

Plaintext message: Green eggs and ham

Shift: 12

Ciphertext: SDQQZQSSEMZPTMY

## Decryption:

Ciphertext message: SDQQZQSSEMZPTMY

Shift 12:

Plaintext: GREENEGGSANDHAM

The Caesar cipher is outfitted with input validation so the message will only accept letters and the shift value will only accept numbers 0-25.  
  
3rd party verification: https://planetcalc.com/1434/

# Hill Cipher:

3rd party verification: <https://planetcalc.com/3327/>

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Message (Plaintext)** | **Key** | **Ciphertext** |
| **1** | [0, 2, 19] | [6, 24, 1, 13, 16, 10, 20, 17, 15] | poh |
| **2** | [0, 2, 19, 15, 14, 7] | [6, 24, 1, 13, 16, 10, 20, 17, 15] | pohrvt |
| **3** | actpoh | GYBNQKURP | pohrvt |
| **4** | gfgidk | Hill magic | swkiuo |
| **5** | magicmessage | trymethis | iykguciucqwq |
| **6** | magicmessage | Try me this | iykguciucqwq |
| **7** | anoddnum | testingss | sasrqukvw |
| **8** | An odd num | testingss | sasrqukvw |

For encryption: pick and enter any of the above keys and enter in one of the messages that shares a row with it. The result should be the ciphertext on that row.

For decryption: pick and enter any of the above ciphertexts. Enter in the key from that row and then the ciphertext. The result should be the plaintext (without spaces) from that row

Data validation notes: All inputs can be entered as strings of letters or 1D arrays consisting only of numbers. Any other configuration will lead to the program re-prompting you for the input. Arrays and strings can be entered with or without spaces and are not case dependent. Keys must fit into a 3 x 3 matrix (9 letters or 9 numbers). Messages can be of any length, but ‘x’ will be added to the end for block sizing if the length of the message is not a multiple of 3.

NOTE: row 7 and 8 demonstrates handling of incomplete blocks. To properly verify run the plaintext ‘anoddnumx’

# Monoalphabetic Cipher:

3rd party verification: <https://www.dcode.fr/monoalphabetic-substitution>

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Message (Plaintext)** | **Key** | **Ciphertext** |
| **1** | This is a test of the system | qwertyuiopasdfghjklzxcvbnm | ziololqztlzgyzitlnlztd |
| **2** | Thisisatestofthesystem | qwertyuiopasdfghjklzxcvbnm | ziololqztlzgyzitlnlztd |
| **3** | alphabeticsoup | zxcvbnmqwertyuiopasdfghjkl | ztoqzxbdwcsifo |
| **4** | ALPHABETIC SOUP | zxcvbnmqwertyuiopasdfghjkl | ztoqzxbdwcsifo |
| **5** | CARLYNEEDSTOGRADUATE | mnbvcxzlkjhgfdsapoiuytrewq | bmogwdccviuszomvymuc |
| **6** | Carly needs to graduate | mnbvcxzlkjhgfdsapoiuytrewq | bmogwdccviuszomvymuc |

For encryption: pick and enter any of the above keys and enter in one of the messages that shares a row with it. The result should be the ciphertext on that row.

For decryption: pick and enter any of the above ciphertexts. Enter in the key from that row and then the ciphertext. The result should be the plaintext (without spaces) from that row

Data validation notes: The key entered must be 26 letters in length or the program will re-prompt you to enter it. Keys can only be letters, same goes for plaintexts and ciphertexts. Letters can’t be repeated in the key.

# Playfair Cipher:

## Encryption:

Key: Waldo

Plaintext message: Where is Waldo

Ciphertext: BPKXCKPDLDOW

## Decryption:

Key: Waldo

Ciphertext message: BPKXCKPDLDOW

Plaintext: WHEREISWALDO

Input Validation Notes: the Playfair cipher is outfitted with input validation so the message and key will only accept letters.

3rd party verification: https://planetcalc.com/7751/

# S-DES Cipher:

## Encryption:

10-bit key: 0101010101

8-bit message: 10101010

Ciphertext: 00101010

## Decryption:

10-bit key: 0101010101

8-bit message: 00101010

Plaintext: 10101010

The S-DES is outfitted with input validation so the key will only accept input that is binary and 10 bits in length. The message will only accept binary and 8 bits in length.

3rd Party verification: https://fauzanakmalh1.github.io/Simplified-DES-Calculator/

# Vigenère Cipher:

3rd party verification: <https://cryptii.com/pipes/vigenere-cipher>

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Message (Plaintext)** | **Key** | **Ciphertext** |
| **1** | This is a test of the system | d k n | wrvvsfddrvdbiduhclvdrp |
| **2** | Thisisatestofthesystem | dkn | wrvvsfddrvdbiduhclvdrp |
| **3** | This is a test of the system | DKN | wrvvsfddrvdbiduhclvdrp |
| **4** | Thisisatestofthesystem | D K N | wrvvsfddrvdbiduhclvdrp |
| **5** | This is a test of the system | (3, 10, 13) | wrvvsfddrvdbiduhclvdrp |
| **6** | Thisisatestofthesystem | (3, 10, 13) | wrvvsfddrvdbiduhclvdrp |
| **7** | asecretmessage | spystuff | shcukyyrwhqszy |
| **8** | A secret message | Spy stuff | shcukyyrwhqszy |
| **9** | Please like our project | iwannapass | xhenfeaicwwqrceoyeul |
| **10** | pleaselikeourproject | I wanna pass | xhenfeaicwwqrceoyeul |

For encryption: pick and enter any of the above keys and enter in one of the messages that shares a row with it. The result should be the ciphertext on that row.

For decryption: pick and enter any of the above ciphertexts. Enter in the key from that row and then the ciphertext. The result should be the plaintext (without spaces) from that row

Data validation notes: The program will force you to re-enter any messages that are numbers for ciphertext or plaintext. It will also only accept keys that are comprised of letters or are in tuple form ( #, #) for any length tuple that contains only digits.