

14. Write a python program for one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

Code:

```
import random

import string

# Function to generate random key for OTP

def generate_key(length):

    return [random.randint(0, 25) for _ in range(length)]

# Function to encrypt using One-Time Pad Vigenere

def otp_encrypt(plaintext, key):

    plaintext = plaintext.lower().replace(" ", "")

    ciphertext = ""

    for i in range(len(plaintext)):

        p = ord(plaintext[i]) - ord('a')

        c = (p + key[i]) % 26

        ciphertext += chr(c + ord('a'))

    return ciphertext

# Function to decrypt

def otp_decrypt(ciphertext, key):

    plaintext = ""

    for i in range(len(ciphertext)):

        c = ord(ciphertext[i]) - ord('a')

        p = (c - key[i]) % 26

        plaintext += chr(p + ord('a'))

    return plaintext
```

```

# ----- MAIN PROGRAM -----

plaintext = "attack at once"

# Remove spaces

pt = plaintext.replace(" ", "")

# Generate key (same length as plaintext)

key = generate_key(len(pt))

cipher = otp_encrypt(pt, key)

decrypted = otp_decrypt(cipher, key)

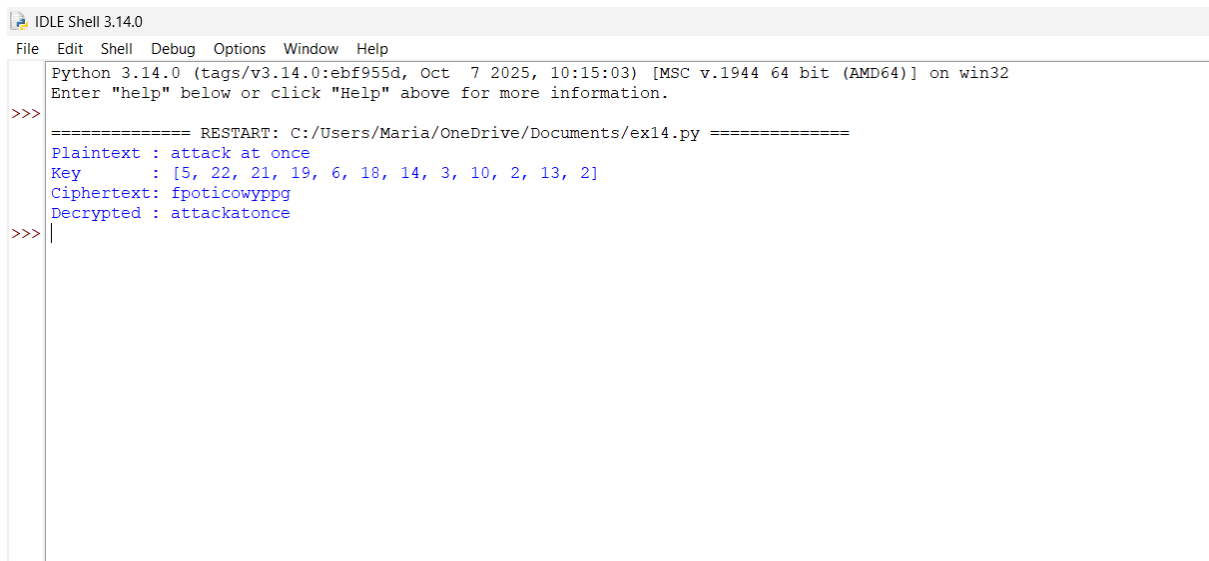
print("Plaintext :", plaintext)

print("Key      :", key)

print("Ciphertext:", cipher)

print("Decrypted :", decrypted)

```



```

IDLE Shell 3.14.0
File Edit Shell Debug Options Window Help
Python 3.14.0 (tags/v3.14.0:ebf955d, Oct 7 2025, 10:15:03) [MSC v.1944 64 bit (AMD64)] on win32
Enter "help" below or click "Help" above for more information.
>>>
===== RESTART: C:/Users/Maria/OneDrive/Documents/ex14.py =====
Plaintext : attack at once
Key       : [5, 22, 21, 19, 6, 18, 14, 3, 10, 2, 13, 2]
Ciphertext: fpoticowyppg
Decrypted : attackatonce
>>>

```