35. 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
def generate_key(length):
    """Generate a random key: list of integers 0-26"""
    return [random.randint(0, 26) for _ in range(length)]
def encrypt(plaintext, key):
    """Encrypt plaintext using one-time pad Vigenère cipher"""
    plaintext = plaintext.upper()
    ciphertext = ""
    for i, char in enumerate(plaintext):
        if char in string.ascii_uppercase:
            shift = key[i]
            cipher_char = chr((ord(char) - ord('A') + shift) % 26 + ord('A'))
            ciphertext += cipher_char
        else:
            ciphertext += char  # keep non-letter as is
    return ciphertext
def decrypt(ciphertext, key):
    """Decrypt ciphertext using one-time pad Vigenère cipher"""
    plaintext = ""
    for i, char in enumerate(ciphertext):
        if char in string.ascii_uppercase:
            shift = key[i]
```

```
            plain_char = chr((ord(char) - ord('A') - shift) % 26 + ord('A'))
            plaintext += plain_char
        else:
            plaintext += char
    return plaintext
# -------------------------
# Example usage
# -------------------------
plaintext = "MEET ME AT NOON"
key = generate_key(len(plaintext))
ciphertext = encrypt(plaintext, key)
decrypted = decrypt(ciphertext, key)
print("Plaintext :", plaintext)
print("Random Key:", key)
print("Ciphertext:", ciphertext)
print("Decrypted :", decrypted)
```

```
>>>
========== RESTART: C:/Users/Maria/OneDrive/Documents/ex35.py ==========
Plaintext : MEET ME AT NOON
Random Key: [5, 4, 7, 0, 19, 17, 3, 14, 17, 24, 15, 20, 19, 25, 23]
Ciphertext: RILT DH RR HHNK
Decrypted : MEET ME AT NOON
>>>
```