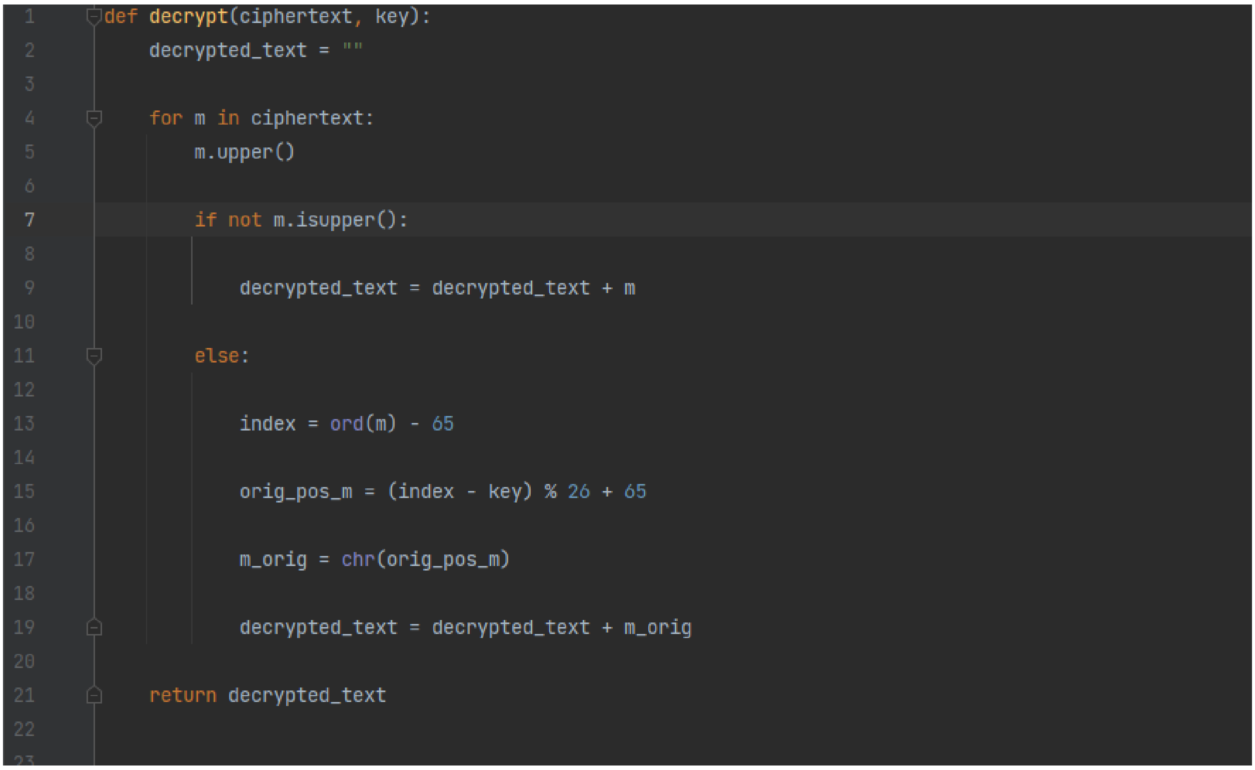
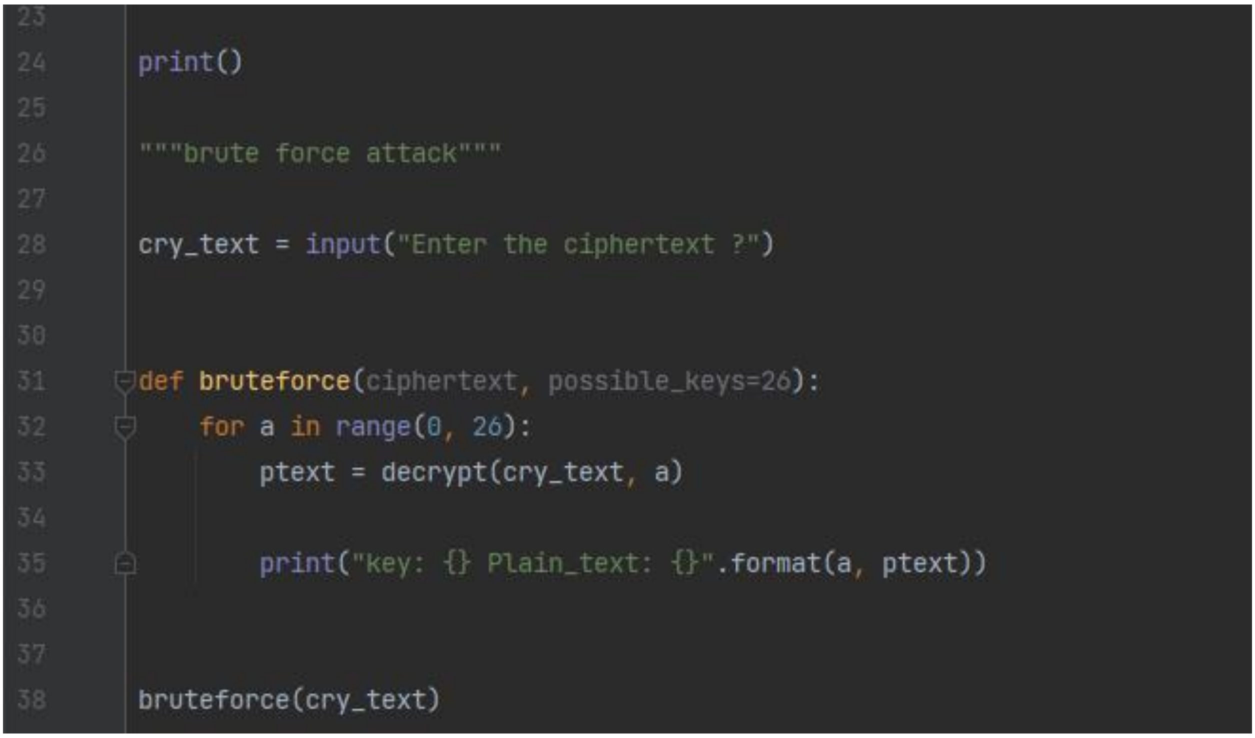
CS458- Assignment -1

Ques: -Write a Java/python program that performs a brute force attack on shift cipher.



```python
def decrypt(ciphertext, key):
    decrypted_text = ""

    for m in ciphertext:
        m.upper()

        if not m.isupper():

            decrypted_text = decrypted_text + m

        else:

            index = ord(m) - 65

            orig_pos_m = (index - key) % 26 + 65

            m_orig = chr(orig_pos_m)

            decrypted_text = decrypted_text + m_orig

    return decrypted_text

```



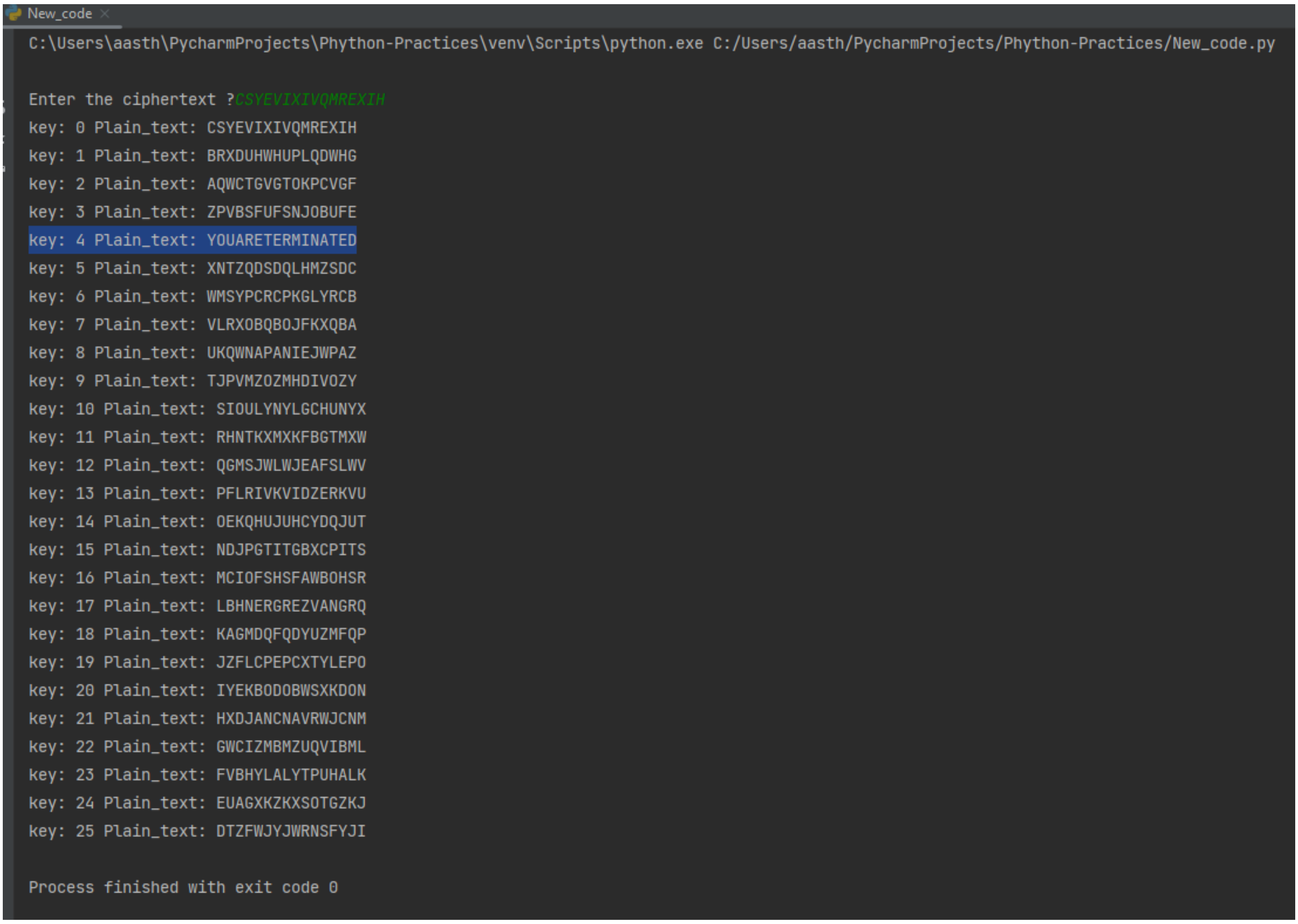
```python

print()

"""brute force attack"""

cry_text = input("Enter the ciphertext ?")


def bruteforce(ciphertext, possible_keys=26):
    for a in range(0, 26):
        ptext = decrypt(cry_text, a)

        print("key: {} Plain_text: {}".format(a, ptext))


bruteforce(cry_text)
```

Output: -

Key = 4

Encrypted Text = CSYEVIXIVQMREXIH

Decrypted Text = You are terminated



```
C:\Users\aasth\PycharmProjects\Phython-Practices\venv\Scripts\python.exe C:/Users/aasth/PycharmProjects/Phython-Practices/New_code.py

Enter the ciphertext ?CSYEVIXIVQMREXIH
key: 0 Plain_text: CSYEVIXIVQMREXIH
key: 1 Plain_text: BRXDUHWHUPLQDWHG
key: 2 Plain_text: AQWCTGVGTOKPCVGF
key: 3 Plain_text: ZPVBSFUFSNJOBUFE
key: 4 Plain_text: YOUARETERMINATED
key: 5 Plain_text: XNTZQDSDQLHMZSDC
key: 6 Plain_text: WMSYPCRCPKGLYRCB
key: 7 Plain_text: VLRXOBQBOJFKXQBA
key: 8 Plain_text: UKQWNAPANIEJWPAZ
key: 9 Plain_text: TJPVMZOZMHDIVOZY
key: 10 Plain_text: SIOULYNYLGCHUNYX
key: 11 Plain_text: RHNTKXMXKFBGTMXW
key: 12 Plain_text: QGMSJWLWJEAFSLWV
key: 13 Plain_text: PFLRIVKVIDZERKVU
key: 14 Plain_text: OEKQHUJUHCYDQJUT
key: 15 Plain_text: NDJPGTITGBXCPITS
key: 16 Plain_text: MCIOFSHSFAWBOHSR
key: 17 Plain_text: LBHNERGREZVANGRQ
key: 18 Plain_text: KAGMDQFQDYUZMFQP
key: 19 Plain_text: JZFLCPEPCXTYLEPO
key: 20 Plain_text: IYEKBODOBWSXKDON
key: 21 Plain_text: HXDJANCNAVRWJCNM
key: 22 Plain_text: GWCIZMBMZUQVIBML
key: 23 Plain_text: FVBHYLALYTPUHALK
key: 24 Plain_text: EUAGXKZKXSOTGZKJ
key: 25 Plain_text: DTZFWJYJWRNSFYJI

Process finished with exit code 0
```

Terminology

Here m is a letter in a sequence of letters.

Ciphertext refers to the encrypted text, which we are going to decode and convert into a simple sentence or words used in the common English language.

The code above is a simple code to demonstrate how brute force attack works. We will first decrypt the code using the function decrypt. We will apply the formula for decrypting the word/sentence and, after that, we can apply a brute-force attack. I have made it a separate function named bruteforce by using function declaration syntax def.

Submitted By: -

Aastha Dhir

CWID- A20468022

adhir2@hawk.iit.edu