Affine and Vigenère Cryptosystem

In this assignment, I have designed two cryptosystems:

- *Affine Cryptosystem*
- *Vigenère Cryptosystem*

The program consists of

- 2 dictionaries:
    - *dictionaryAlphaToNum*: It is a dictionary consisting of Alphabets and their corresponding numeric values. This helps me convert a given alphabet to a number and avoid any duplications.
    - *dictionayNumToAlpha*: It is a dictionary consisting of Numbers and their corresponding Alphabetic values. This helps me convert a given Number to an Alphabet and avoid any duplications.
- 7 functions (3 functions for Vigenère Cipher, 3 functions for Affine and 1 main function)
    - *vTable(listChoice)*: This function acts like a Vigenère table. The function takes in *listChoice* as a parameter which is of type char. It helps the program chose a row from the Vigenère table. The lists are made in accordance with the Vigenère table.
    - *encryptVigenere(messageList,key)*: This function is the encryption Function for Vigenère cipher. It takes two parameters, *messageList* which is a list that consists of characters of the plaintext message in the order of input and *key* which is a list of characters of the key in the order of input. It returns the encrypted string which of string type.
    - *decryptVigenere(cipherList,key):* This function is the encryption Function for Vigenère cipher. It takes two parameters, *cipherList* which is a list that consists of characters of the ciphertext message in the order of input and *key* which is a list of characters of the key in the order of input. It returns the decipherMessage which of string type.
    - *encryptAffine(plaintext,a,b):* This function is the encryption Function for Vigenère cipher. It takes three parameters, *plainText* which is a list that consists of characters of the plaintext message in the order of input, *a* which is the A coefficient and b which is the b coefficient. It returns cipherMessage which is of string type.

- decryptAffine(cipher,a,b): This function is the encryption Function for Vigenère cipher. It takes three parameters, *cipher* which is a list that consists of characters of the cipher message in the order of input, *a* which is the A coefficient and b which is the b coefficient. It returns cipherMessage which is of string type.
- *multInverse(num1, num):* It is a function that is used to generate Multiplicative Modulo Inverse of a number. I used the following formula, ***num1*itr = 1 mod num2.*** There are two parameters, *num1* which is the number whose inverse we are calculating and *num2* which is our number which when divided by the product of our original number and the inverse will yield a remainder 1.
- *Main():* The driver function for the program. It is responsible for printing, taking user input and output the plaintext and cipher text.

Sample Input and output

Note: ***The plaintext should be an alphabetical string with no spaces. The key for Vigerene cipher should also be an alphabetical string with no spaces while the two keys A and B for Affine cipher should be coprime numbers.***

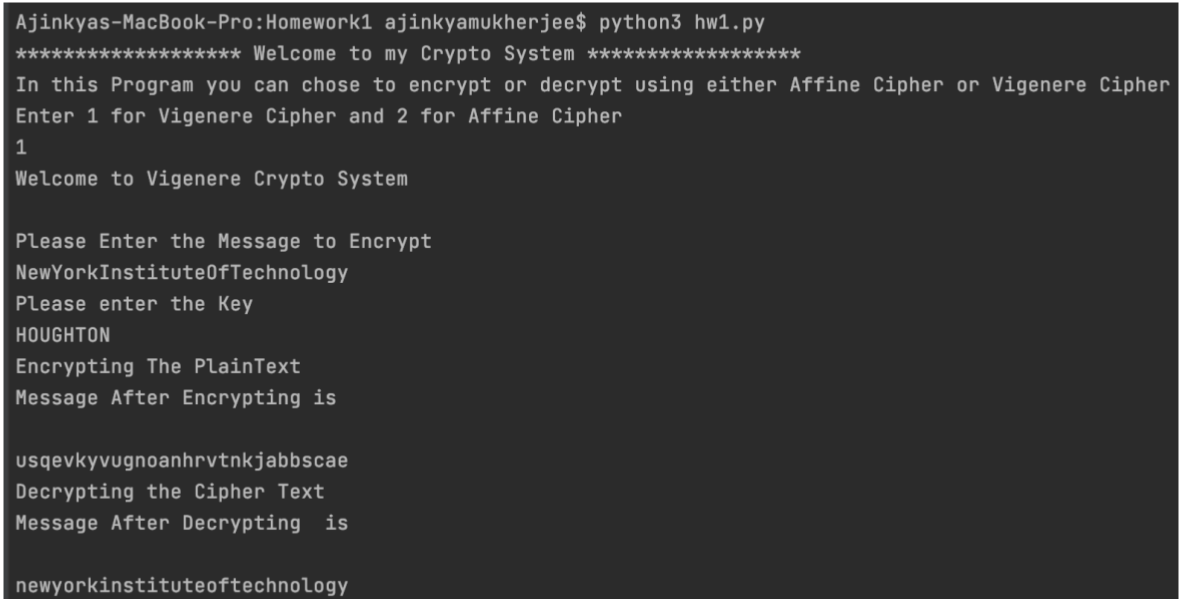
In this section I have pasted screenshots of input and outputs used to check the working of cryptosystem.

To compile the code simply type: ***python3 crypto.py***

Sample Inputs and Corresponding outputs

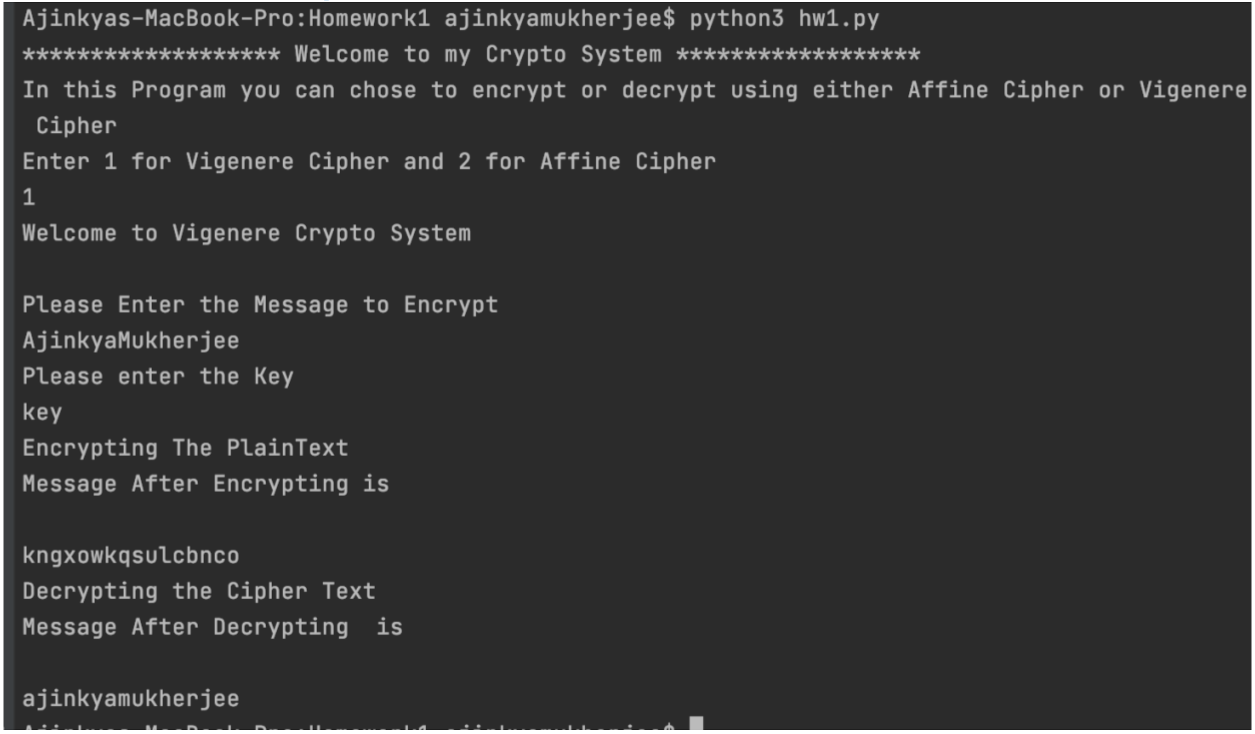
1. Vigenère Cipher

Input 1: Plaintext: *NewYorkInstituteOfTechnology*
Key: *HOUGHTON*



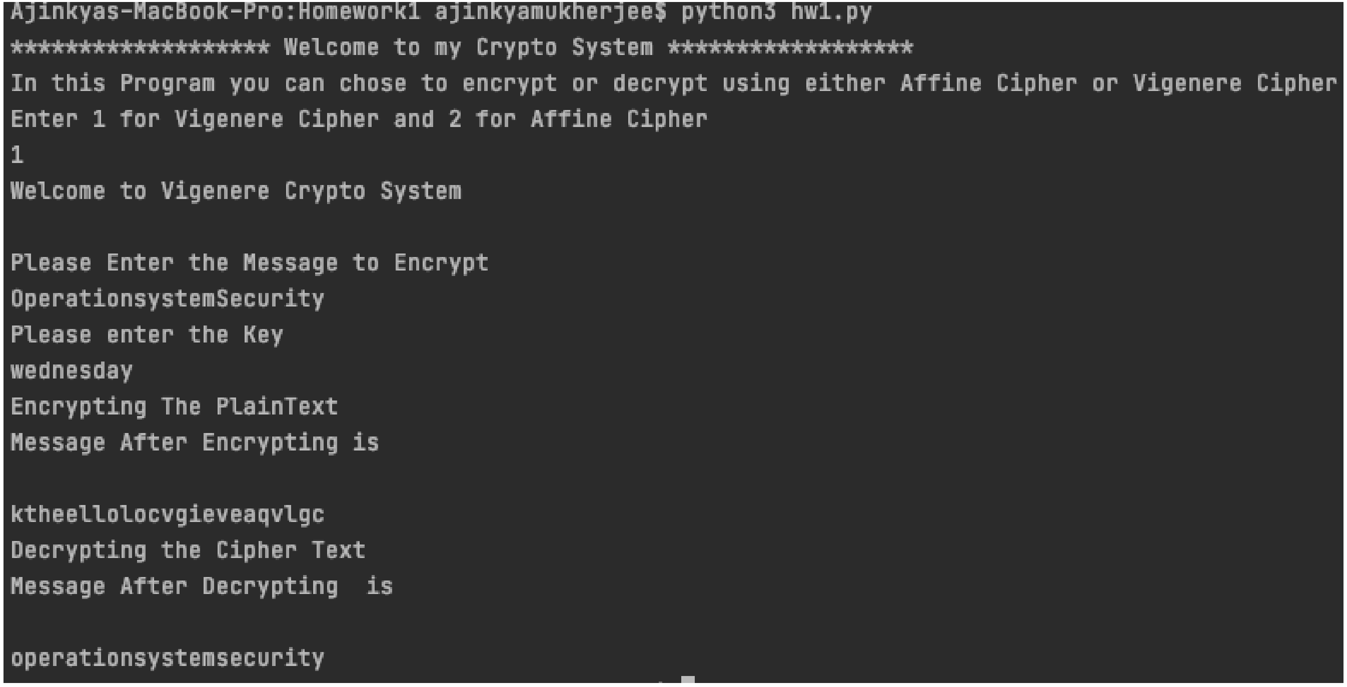
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
****************** Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
1
Welcome to Vigenere Crypto System

Please Enter the Message to Encrypt
NewYorkInstituteOfTechnology
Please enter the Key
HOUGHTON
Encrypting The PlainText
Message After Encrypting is

usqevkyvugnoanhrvtnkjabbscae
Decrypting the Cipher Text
Message After Decrypting  is

newyorkinstituteoftechnology
```

Input 2: Plaintext: *AjinkyaMukherjee*
Key: *key*



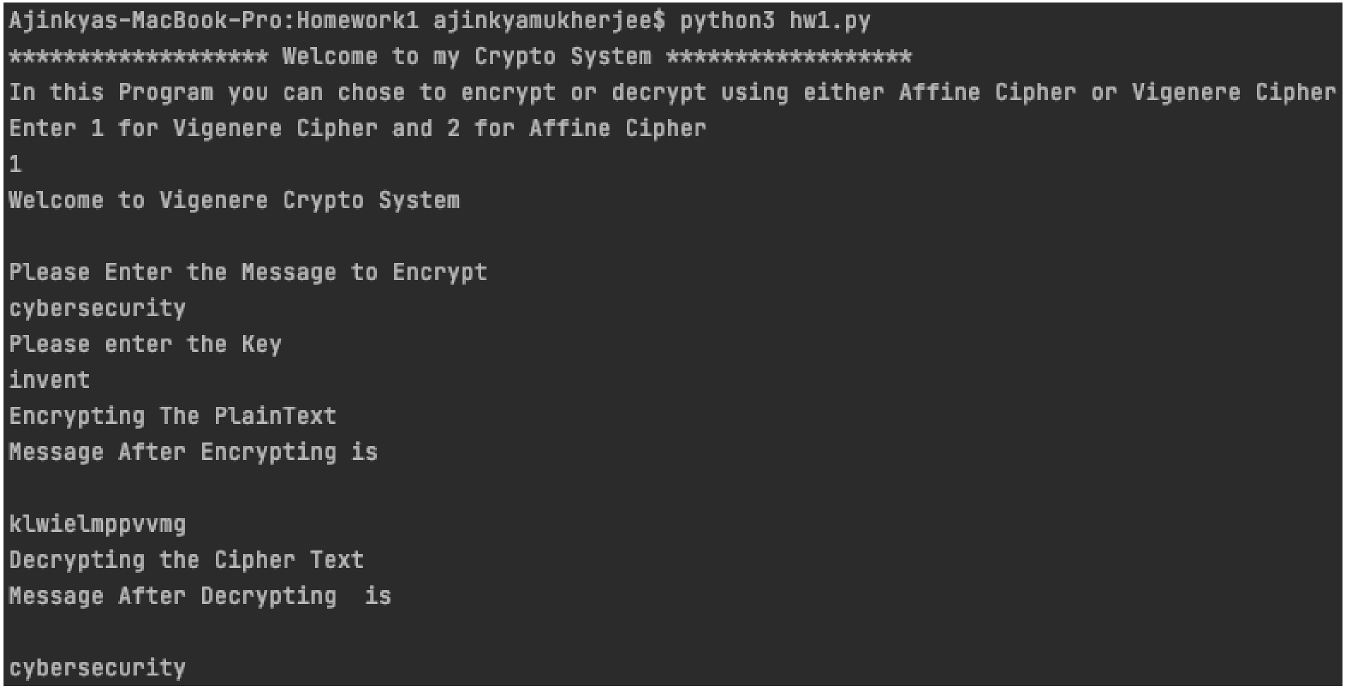
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
****************** Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere
 Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
1
Welcome to Vigenere Crypto System

Please Enter the Message to Encrypt
AjinkyaMukherjee
Please enter the Key
key
Encrypting The PlainText
Message After Encrypting is

kngxowkqsulcbnco
Decrypting the Cipher Text
Message After Decrypting  is

ajinkyamukherjee
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$
```

Input 3: Plaintext: *OperationsystemSecurity*
Key: *Wednesday*



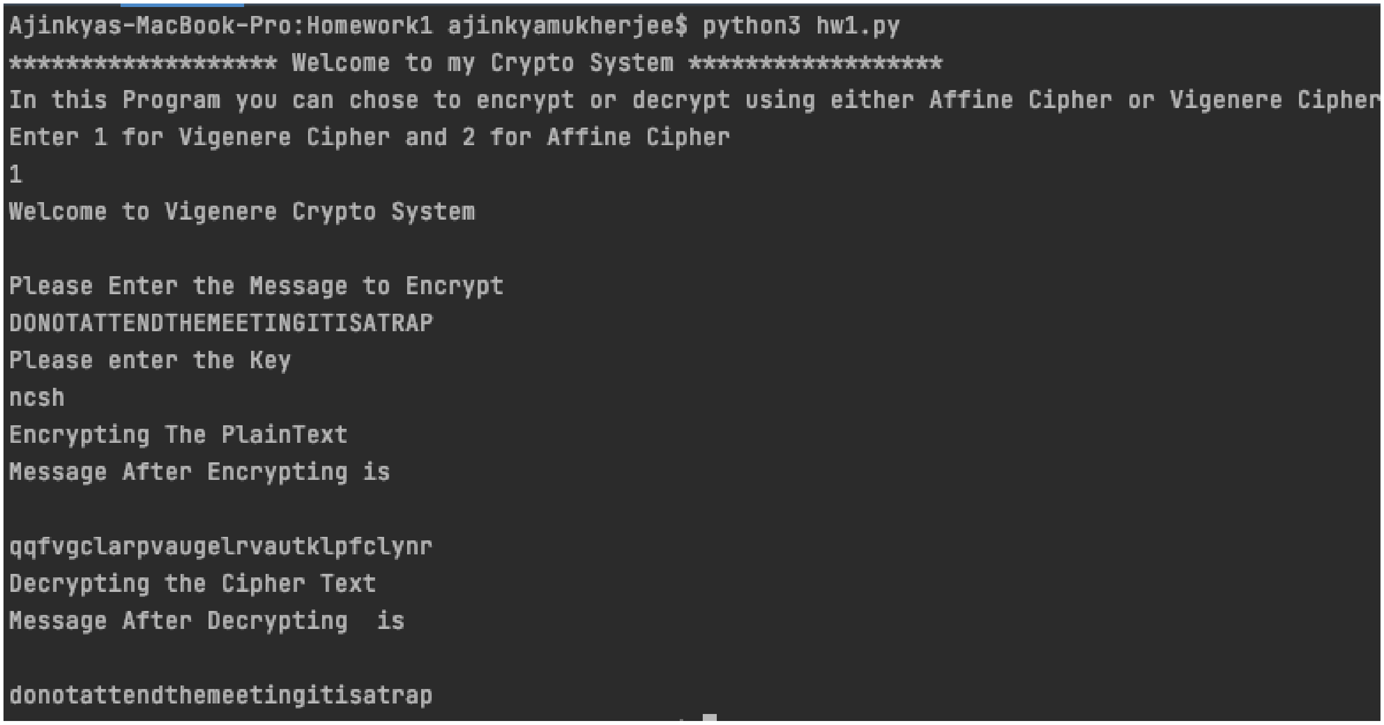
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
1
Welcome to Vigenere Crypto System

Please Enter the Message to Encrypt
OperationsystemSecurity
Please enter the Key
wednesday
Encrypting The PlainText
Message After Encrypting is

ktheellolocvgieveaqvlgc
Decrypting the Cipher Text
Message After Decrypting  is

operationsystemsecurity
```

Input 4: Plaintext: *cybersecurity*
Key: *INVENT*



```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
1
Welcome to Vigenere Crypto System

Please Enter the Message to Encrypt
cybersecurity
Please enter the Key
invent
Encrypting The PlainText
Message After Encrypting is

klwielmppvvmg
Decrypting the Cipher Text
Message After Decrypting  is

cybersecurity
```

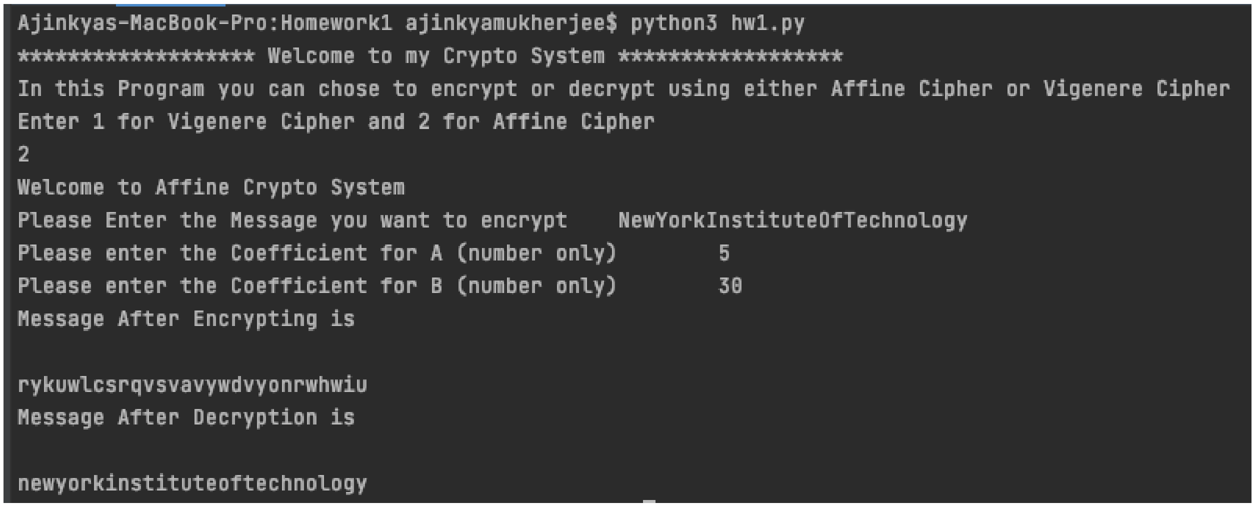
Input 5: plaintext: *DONOTATTENDTHEMEETINGITISATRAP*
Key: *ncsh*



```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
1
Welcome to Vigenere Crypto System

Please Enter the Message to Encrypt
DONOTATTENDTHEMEETINGITISATRAP
Please enter the Key
ncsh
Encrypting The PlainText
Message After Encrypting is

qqfvgclarpvaugelrvautklpfclynr
Decrypting the Cipher Text
Message After Decrypting  is

donotattendthemeetingitisatrap
```

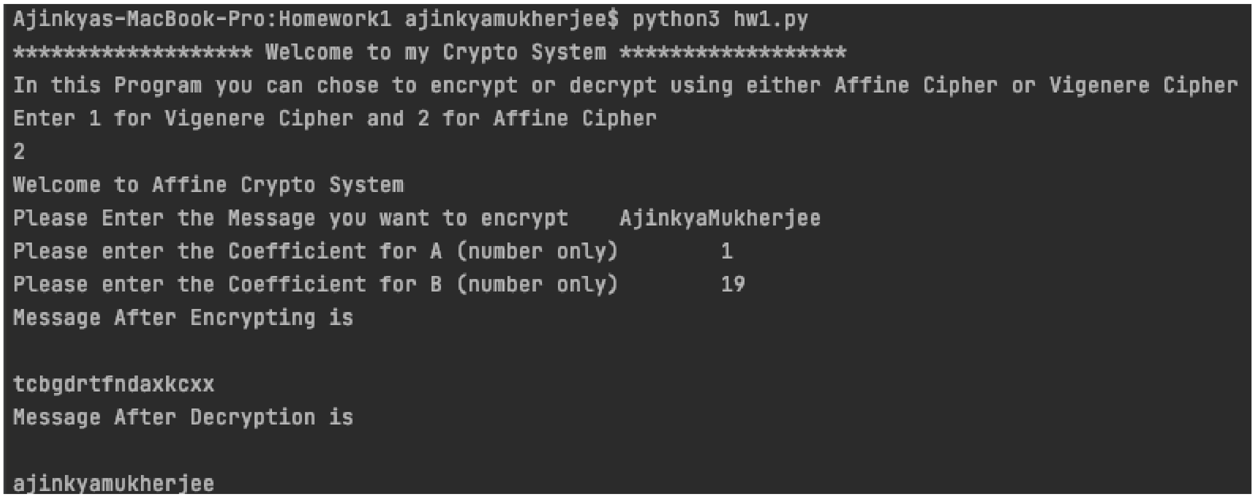
2. Affine Cipher

Input 1: Plaintext: *NewYorkInstituteOfTechnology*
A Coefficient: 5
B Coefficient: 30



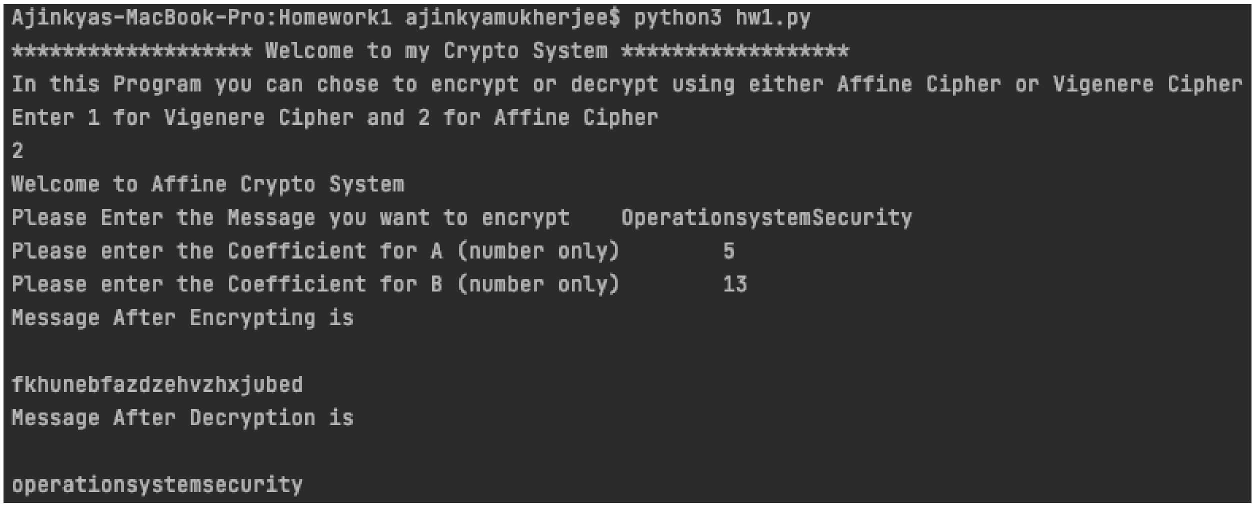
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
2
Welcome to Affine Crypto System
Please Enter the Message you want to encrypt    NewYorkInstituteOfTechnology
Please enter the Coefficient for A (number only)        5
Please enter the Coefficient for B (number only)        30
Message After Encrypting is

rykuwlcsrqvsvavywdvyonrwhwiu
Message After Decryption is

newyorkinstituteoftechnology
```

```
Input 2: Plaintext: AjinkyaMukherjee
         A Coefficient: 1
         B Coefficient: 19
```



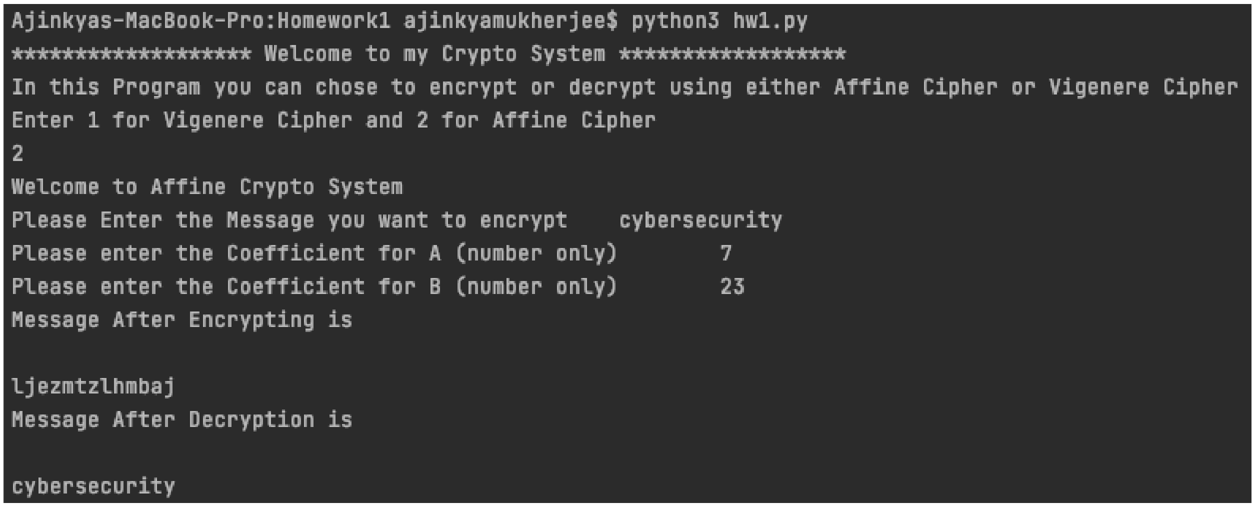
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
2
Welcome to Affine Crypto System
Please Enter the Message you want to encrypt    AjinkyaMukherjee
Please enter the Coefficient for A (number only)        1
Please enter the Coefficient for B (number only)        19
Message After Encrypting is

tcbgdrtfndaxkcxx
Message After Decryption is

ajinkyamukherjee
```

```
Input 3: Plaintext: OperationsystemSecurity
         A Coefficient: 5
         B Coefficient: 13
```



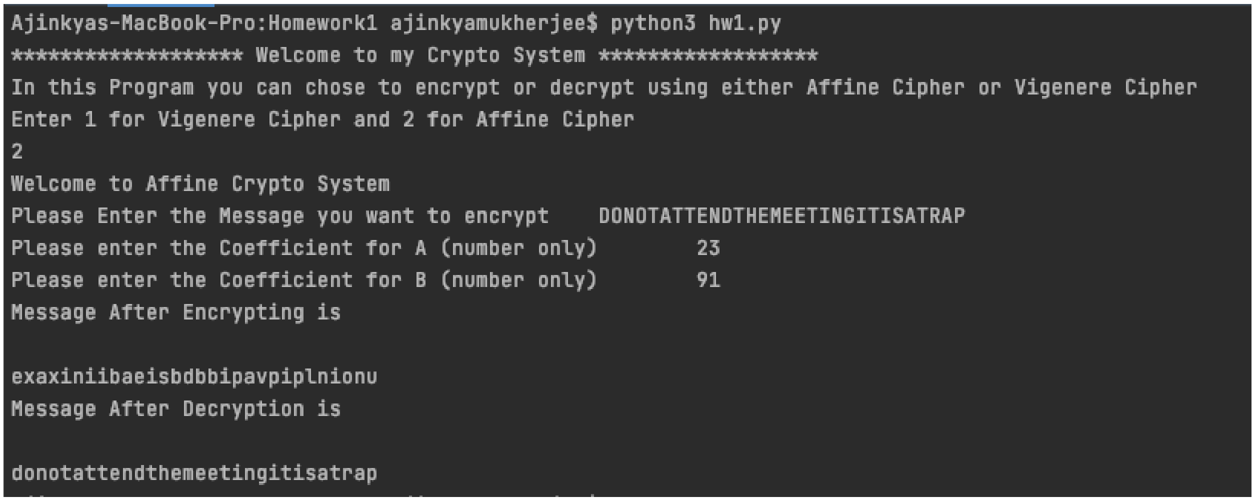
```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
******************* Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
2
Welcome to Affine Crypto System
Please Enter the Message you want to encrypt    OperationsystemSecurity
Please enter the Coefficient for A (number only)        5
Please enter the Coefficient for B (number only)        13
Message After Encrypting is

fkhunebfazdzehvzhxjubed
Message After Decryption is

operationsystemsecurity
```

```
Input 4: Plaintext: cybersecurity
         A Coefficient: 7
         B Coefficient: 23
```



```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
****************** Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
2
Welcome to Affine Crypto System
Please Enter the Message you want to encrypt    cybersecurity
Please enter the Coefficient for A (number only)        7
Please enter the Coefficient for B (number only)        23
Message After Encrypting is

ljezmtzlhmbaj
Message After Decryption is

cybersecurity
```

```
Input 5: Plaintext: DONOTATTENDTHEMEETINGITISATRAP
         A Coefficient: 5
         B Coefficient: 13
```



```
Ajinkyas-MacBook-Pro:Homework1 ajinkyamukherjee$ python3 hw1.py
****************** Welcome to my Crypto System ******************
In this Program you can chose to encrypt or decrypt using either Affine Cipher or Vigenere Cipher
Enter 1 for Vigenere Cipher and 2 for Affine Cipher
2
Welcome to Affine Crypto System
Please Enter the Message you want to encrypt    DONOTATTENDTHEMEETINGITISATRAP
Please enter the Coefficient for A (number only)        23
Please enter the Coefficient for B (number only)        91
Message After Encrypting is

exaxiniibaeisbdbbipavpiplnionu
Message After Decryption is

donotattendthemeetingitisatrap
```

<u>Note</u>: Other plaintexts and keys can be used as long as the following rules are followed.

- ***The plaintext should be an alphabetical string with no spaces.***

- ***The key for Vigerene cipher should also be an alphabetical string with no spaces while the two keys A and B for Affine cipher should be coprime numbers***