APPLIED CRYPTOGRAPHY

Lab 2 : OTP and Cryptanalysis

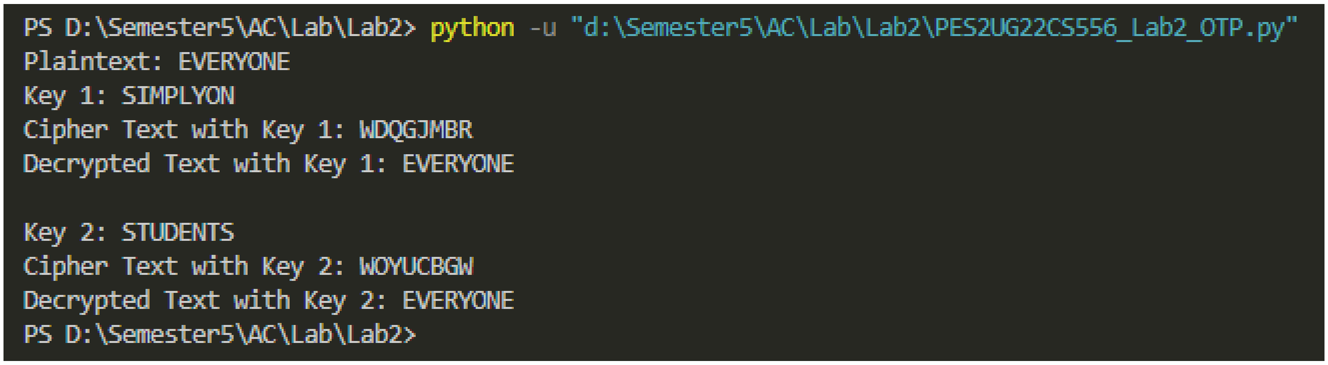
Name: Siri N Shetty SRN: PES2UG22CS556

Problem 1:

a) **OTP Cipher**

(Use Random Key Generation) : Encryption and Decryption

Test for 2 random keys {demonstrate non-repetition and no pattern recognition possible}



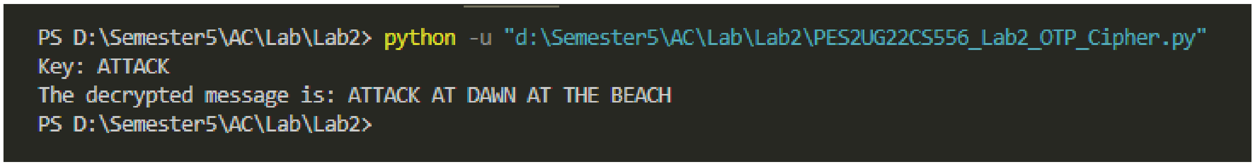
```
PS D:\Semester5\AC\Lab\Lab2> python -u "d:\Semester5\AC\Lab\Lab2\PES2UG22CS556_Lab2_OTP.py"
Plaintext: EVERYONE
Key 1: SIMPLYON
Cipher Text with Key 1: WDQGJMBR
Decrypted Text with Key 1: EVERYONE

Key 2: STUDENTS
Cipher Text with Key 2: WOYUCBGW
Decrypted Text with Key 2: EVERYONE
PS D:\Semester5\AC\Lab\Lab2>
```

b) **Decryption of OTP Cipher**

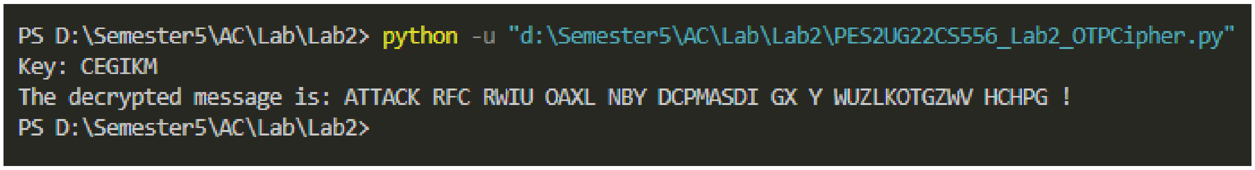
As you were deep into your covert operation, a mysterious transmission was intercepted from a known source. The message reads:
CXZIMW VLK DYMA YMZP VLK HIXWMUHO QJ C EELNOUBQLYZ PMTRK !
You know that the sender always uses OTP cipher and begins his encrypted message with the word ATTACK.

i)What are the first six letters of the key?
ii)How do you think the key might continue?
iii)Decrypt the entire message .

i) The first 5 letters of the key is CEGIKM
ii) But the derived key above won’t work for decrypting the entire message, hence the final key will be ATTACK
iii) The Decrypted message: - ATTACK AT DAWN AT THE BEACH



```
PS D:\Semester5\AC\Lab\Lab2> python -u "d:\Semester5\AC\Lab\Lab2\PES2UG22CS556_Lab2_OTP_Cipher.py"
Key: ATTACK
The decrypted message is: ATTACK AT DAWN AT THE BEACH
PS D:\Semester5\AC\Lab\Lab2>
```



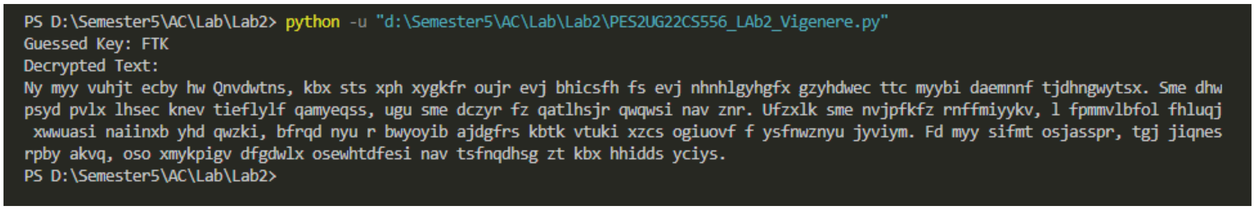
```
PS D:\Semester5\AC\Lab\Lab2> python -u "d:\Semester5\AC\Lab\Lab2\PES2UG22CS556_Lab2_OTPCipher.py"
Key: CEGIKM
The decrypted message is: ATTACK RFC RWIU OAXL NBY DCPMASDI GX Y WUZLKOTGZWV HCHPG !
PS D:\Semester5\AC\Lab\Lab2>
```

Problem 2:

You have intercepted Alice's message and you know that Alice has used Vigenère cipher with a key length of 3 to encrypt the message. Decrypt the cipher-text using frequency analysis. You can use any online frequency analysis tools to help you with this task.
(Note: Preserve the punctuation)

The cipher text is:
Sr rri oemcd xmgr mp Vgfipdsl, dlc cyl cir qildpw yzcb xfo lmbmxyr yc xfo xmgrqzimzpc qerripoh dyv rrigb itorgxk dowrszgdmcc. Xfo wrbicdw uovc vmloh usxf msjyvdep jkrrovlc, eln xfo wmerb yj jkyerxcb jgvpcn xfo egb. Ekshqd xfo gfoippyj kxkywnripo, e kiwrovgyyq pmeevc cpgztcn xfbssql rri absun, gybvw sre k gpitrsg kowqkkc dlyd amepb csmx ylbetop y dlpspjsre ciabir. Kw rri lskfd hcotcxib, dlc obasxcwild kpoa, yxh cfipislo iyqipvc yxxgmmnkxcn xfo ylpsjnmlq sd dlc rmbnil dvsdl.

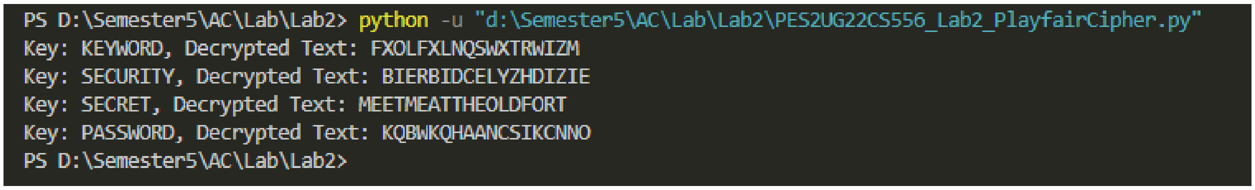
i) The Decrypted message: - **It has come to my attention, that the use of encrypted messages in this context is highly inappropriate. The correct method to address these issues is to communicate directly and securely. Please ensure that all future communications are handled in a transparent and accountable manner. We must adhere to protocols and avoid any further misunderstanding or misuse of sensitive information.**
ii) Key Value: - **HIS**



```
PS D:\Semester5\AC\Lab\Lab2> python -u "d:\Semester5\AC\Lab\Lab2\PES2UG22CS556_LAb2_Vigenere.py"
Guessed Key: FTK
Decrypted Text:
Ny myy vuhjt ecby hw Qnvdwtns, kbx sts xph xygkfr oujr evj bhicsfh fs evj nhnhlgyhgfx gzyhdwec ttc myybi daemnnf tjdhngwytsx. Sme dhw
psyd pvlx lhsec knev tieflylf qamyeqss, ugu sme dczyr fz qatlhsjr qwqwsi nav znr. Ufzxlk sme nvjpfkfz rnffmiyykv, l fpmmvlbfol fhluqj
 xwwuasi naiinxb yhd qwzki, bfrqd nyu r bwyoyib ajdgfrs kbtk vtuki xzcs ogiuovf f ysfnwznyu jyviym. Fd myy sifmt osjasspr, tgj jiqnes
rpby akvq, oso xmykpigv dfgdwlx osewhtdfesi nav tsfnqdhsg zt kbx hhidds yciys.
PS D:\Semester5\AC\Lab\Lab2>
```

Problem 3 : Playfair Cipher

Playfair cipher, was often used for its simplicity and security during World War I and II.
Below is a cipher-text encrypted using Playfair. Perform cryptanalysis and decrypt the message.
(Hint - try using the most commonly used keys)
ITCSITGSSMBWKFBQTS



```
PS D:\Semester5\AC\Lab\Lab2> python -u "d:\Semester5\AC\Lab\Lab2\PES2UG22CS556_Lab2_PlayfairCipher.py"
Key: KEYWORD, Decrypted Text: FXOLFXLNQSWXTRWIZM
Key: SECURITY, Decrypted Text: BIERBIDCELYZHDIZIE
Key: SECRET, Decrypted Text: MEETMEATTHEOLDFORT
Key: PASSWORD, Decrypted Text: KQBWKQHAANCSIKCNNO
PS D:\Semester5\AC\Lab\Lab2>
```

The Decrypted message is: - MEETMEATTHEOLDFORT