**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 18C3175**

**CRYPTANALYSIS AND CYBER DEFENSE WORKBOOK**

# 1. Introduction to Cryptography

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Encryption and Decryption.
* To understand the applications of substitution techniques.
* To understand Symmetric Crypto System.

**Pre-Lab Task:**

1. **Define Cryptography and write any two applications of cryptography**

Sol)one that all of us use frequently, is encrypting communications between us and another system. This is most commonly used for communicating between a client program and a server. Examples are a web browser and webserver, or email client and email server. APPLICATIONS: 1. Digital currencies 2. Computer passwords

1. **What are the different types of Cryptographic Algorithms?**

Sol) \* Symmetric-key algorithms.

\* Asymmetric-key algorithms

\* Symmetric-Key Algorithms for Encryption and Decryption

1. **Mention the cryptographic algorithm used in Blockchain Technology and Gmail**

Sol) Use of Cryptography in Blockchain: Blockchains make use of two types of cryptographic algorithms, asymmetric key algorithms, and hash functions................. Blockchains generally use the SHA-256 hashing algorithm as their hash function.

1. **What is the need for encryption?**

Sol) Encryption helps protect your online privacy by turning personal information into “for your eyes only” messages intended only for the parties that need them — and no one else. You should make sure that your emails are being sent over an encrypted connection, or that you are encrypting each message.

1. **Define symmetric cryptography and Asymmetric cryptography.**

Sol) Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. Asymmetric Encryption is a form of Encryption where keys come in pairs. Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret. Users can "sign" messages by encrypting them with their private keys.

**In-Lab Task:**

**Q1) The Magician Ram changes any English sentences into secret information and changes secret information into original message. He takes different English sentences and changes into ciphertext using his own secret key and decrypts the ciphertext into plaintext. Implement the above task using the concept of Caesar Cipher**

**Sample input1**

*Enter the msg*: GOOD DAY

*Enter key: F*

Sample output

*The encrypted msg is* LTTIIFD

*The decrypted msg is:* GOOD DAY

**Sample input 2**

*Enter the msg*: CAESAR

*Enter key: E*

Sample output

*The encrypted msg is* GEIXEV

*The decrypted msg is:* CAESAR

Sol)

def encrypt(message, key):

encrypted = ""

key = ord(key.upper()) - ord('A')

for char in message.upper():

if char.isalpha():

encrypted += chr((ord(char) - ord('A') + key) % 26 + ord('A'))

else:

encrypted += char

return encrypted

def decrypt(message, key):

decrypted = ""

key = ord(key.upper()) - ord('A')

for char in message.upper():

if char.isalpha():

decrypted += chr((ord(char) - ord('A') - key) % 26 + ord('A'))

else:

decrypted += char

return decrypted

def main():

message = input("Enter the msg: ")

key = input("Enter key: ")

encrypted = encrypt(message, key)

print("The encrypted msg is", encrypted)

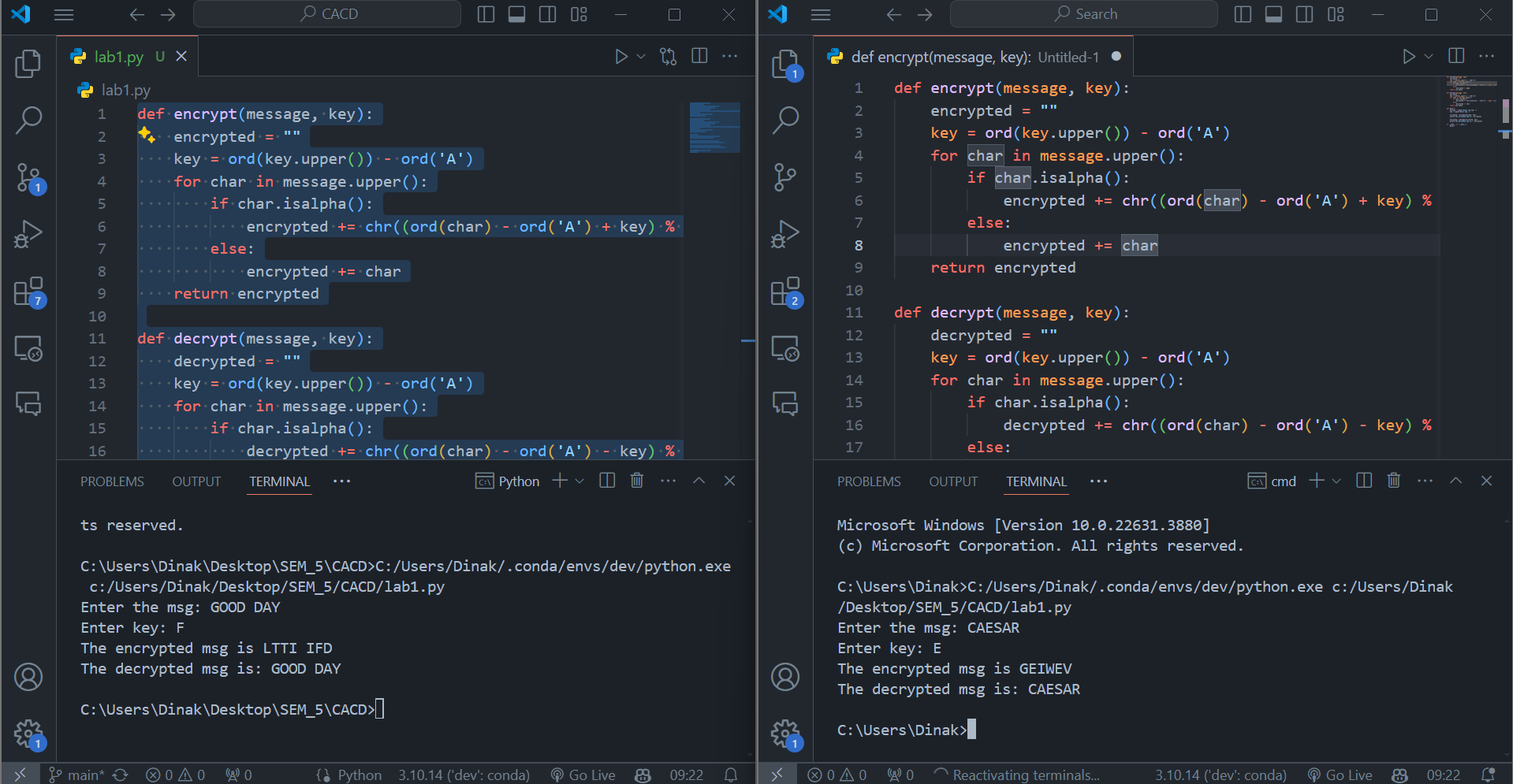
decrypted = decrypt(encrypted, key)

print("The decrypted msg is:", decrypted)

if \_\_name\_\_ == "\_\_main\_\_":

main()

**Output:**



**Post Lab Task:**

**Q2 Hash Include a National Level technical fest has many events, As it is a technical event all the events are designed in technically. One such event is a treasure hunt**

**Rules for the treasure hunt:**

1. **You are given a sheet that consists of alphabets.**
2. **The alphabets in the sheet arranged in a horizontal and vertical row each consist of alphabets from A-Z**

Clue: Substitution Technique of Veigneir Cipher Technique

Sol)

def keys(a,b):

i=0

fkey=""

while(i<len(b)+1):

if(len(fkey)==len(a)):

break

else:

if(i==len(b)):

i=0

fkey=fkey+b[i]

i=i+1

return fkey

def encrypt(txt,key):

res=""

for i in range(len(txt)):

c=txt[i]

d=key[i]

x=(((ord(d)%26)+ord(c))%26)+65

e=chr(x)

res=res+e

return res

def decrypt(txt,key):

res=""

for i in range(len(txt)):

c=txt[i]

d=key[i]

x=((ord(c)-ord(d)+26)%26)+65

e=chr(x)

res=res+e

return res

print("Viginer Ciepher")

print("1.Encrypt")

print("2.Decrypt")

n=int(input("Enter your choice :"))

if(n==1):

a=input("Enter text :")

b=input("Enter Key :")

key=keys(a,b)

d=encrypt(a,key)

print("Ciepher Text :", d)

if(n==2):

a=input("Enter text :")

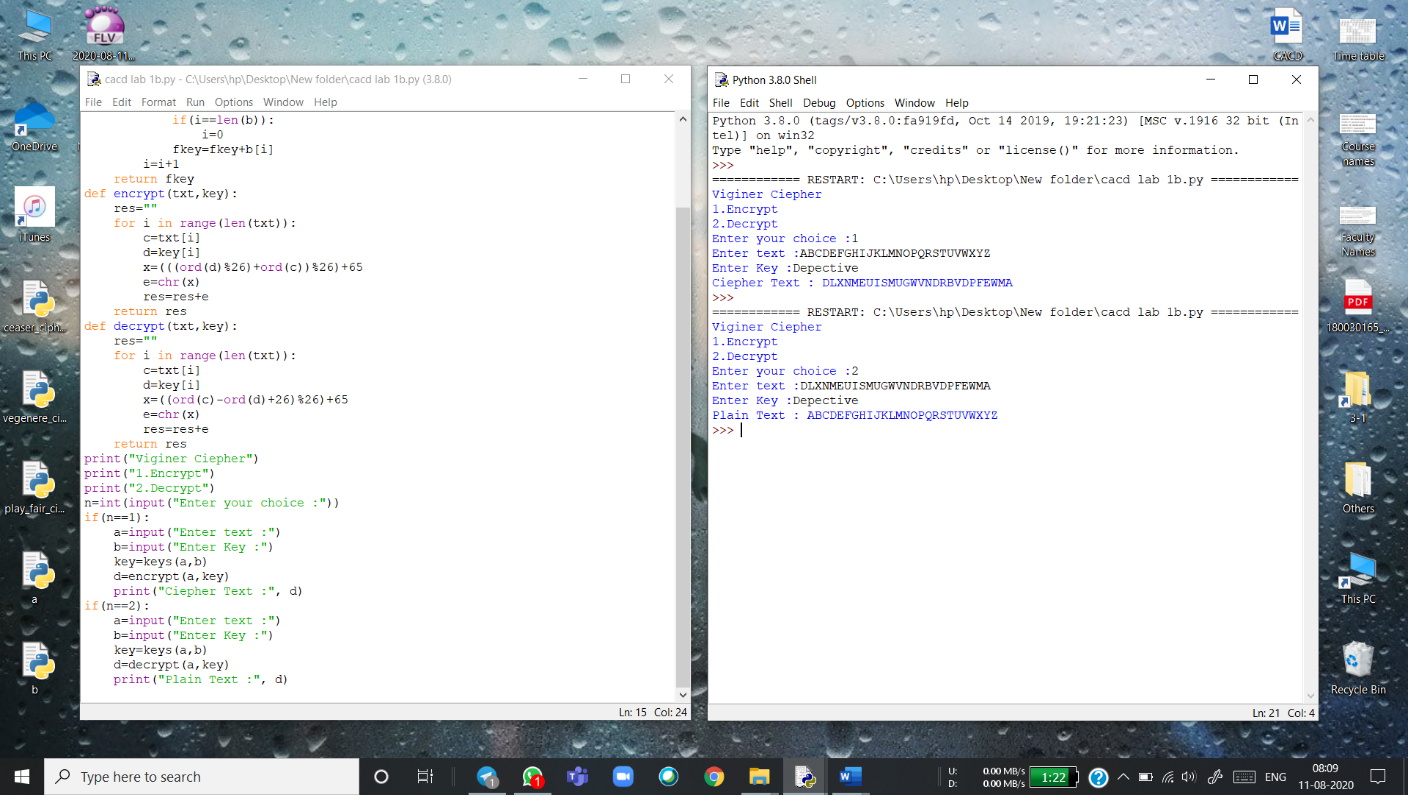
b=input("Enter Key :")

key=keys(a,b)

d=decrypt(a,key)

print("Plain Text :", d)

**Output:**

****