Cryptography

Lab – II

1. WAP for Vigenare Cipher.

Program:

```
def gen(string,key):
    key = list(key)
    if len(string) == len(key):
        return (key)
    else:
        for i in range(len(string)-len(key)):
            key.append(key[i % len(key)])
    return ("".join(key))


def Encrypt(string,key):
    text = []
    for i in range(len(string)):
        X = (ord(string[i])+ord(key[i])) % 26
        X += ord('A')
        text.append(chr(X))
    return ("".join(text))

def Decrypt(text,key):
    plaintext = []
    for i in range(len(text)):
        Y =(ord(text[i])-ord(key[i]) +26) % 26
        Y += ord('A')
        plaintext.append(chr(Y))
    return("".join(plaintext))

if __name__ == "__main__":

    entered_text = input("Enter the text: ")
    entered_key = input("Enter the key: ")
    key = gen(entered_text,entered_key)
    text = Encrypt(entered_text,key)
    dec = Decrypt(text,key)
```

```
    print(f"The encrypted text is: {text}")
    print(f"The decrypted text is: {dec}")
```

Output:

```
PS C:\Users\ashwi\Desktop\lab sem 5> & C:/Users/ashwi/AppData/Local/Programs/Python/Python39/python.exe "c:/Users/ashwi/Desktop/lab sem 5/vineger cipher.py"
Enter the text: ASHWIN
Enter the key: QWEVR
The encrypted text is: QOLRZD
The decrypted text is: ASHWIN
PS C:\Users\ashwi\Desktop\lab sem 5>
```

2. WAP for One Time Pad

Program:

```
import random

def generate(length):
    position_key = [random.randint(0, 25) for i in range(length)]
    key = [chr(place+97) for place in position_key]
    print('Random key: ')
    print(''.join(key))
    return position_key

plaintext = str(input("Ente the plaintext: "))
plaintext = plaintext.lower()
plaintext = plaintext.replace(" ", "")

position_key = generate(len(plaintext))


def Encrypt():
    position_plain = [(ord(char)-97) for char in plaintext]

    ciphertext = list()
```

```
    ciphertext = [(chr(((position_key[i]+position_plain[i]) % 26)+97))
                  for i in range(len(position_plain))]
    return ciphertext

def Decrypt(ciphertext):
    cipherposition  = [(ord(char)-97) for char in ciphertext]

    plaintext = list()
    plaintext = [(chr(((cipherposition[i]-position_key[i]) % 26)+97))
                  for i in range(len(cipherposition))]
    return plaintext

ciphertext=Encrypt()
print("\nThe encrypted text is: ")
print(''.join(ciphertext))

plaintext=Decrypt(ciphertext)
print("\nThe decrypted text is: ")
print(''.join(plaintext))
```

Output: