Name :- Kaustubh Shrikant Kabra

CLass:- TE Computer

ERP :-38

Subject :-LP2(IS) (AES)

Code:-

```
import hashlib
from base64 import b64decode, b64encode

from Crypto import Random
from Crypto.Cipher import AES


class AESCipher(object):
    def __init__(self, key):
        self.block_size = AES.block_size
        self.key = hashlib.sha256(key.encode()).digest()

    def encrypt(self, plain_text):
        plain_text = self.__pad(plain_text)
        iv = Random.new().read(self.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        encrypted_text = cipher.encrypt(plain_text.encode())
        return b64encode(iv + encrypted_text).decode("utf-8")

    def decrypt(self, encrypted_text):
        encrypted_text = b64decode(encrypted_text)
        iv = encrypted_text[:self.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        plain_text = cipher.decrypt(encrypted_text[self.block_size:]).decode("utf-8")
        return self.__unpad(plain_text)

    def __pad(self, plain_text):
        number_of_bytes_to_pad = self.block_size - len(plain_text) % self.block_size
        ascii_string = chr(number_of_bytes_to_pad)
        padding_str = number_of_bytes_to_pad * ascii_string
        padded_plain_text = plain_text + padding_str
        return padded_plain_text

    @staticmethod
    def __unpad(plain_text):
        last_character = plain_text[len(plain_text) - 1:]
        return plain_text[:-ord(last_character)]


key = input("Enter Key: ")
aes = AESCipher(key)
```

```
flag = 1
while flag == 1:
   print("/**************MENU**************/")
   print("1. Encryption")
   print("2. Decryption")
   print("3. Exit ")
   choice = int(input("Enter your choice : "))

   if choice == 1:
      message = input("Enter message to encrypt: ")
      encryptedMessage = aes.encrypt(message)
      print("Encrypted Message:", encryptedMessage)

   elif choice == 2:
      message = input("Enter message to decrypt: ")
      decryptedMessage = aes.decrypt(message)
      print("Decrypted Message:", decryptedMessage)
   elif choice == 3:
      print("Exit")
      flag = 0
   else:
      print("Wrong Choice,Please Choose Another Option.")
```

Output:-

Enter Key: AISSMSIOIT

/**************MENU**************/

1. Encryption

2. Decryption

3. Exit

Enter your choice : 1

Enter Message to Encrypt: Its KK29 aka Kaustubh

Encrypted Message:
K4qVJgSw3vwuRZnUD5YEzVHk41HP796bfHGz7iKNAt1MyLxjzsAUyE7p+5Ape5xo

/**************MENU**************/

1. Encryption

2. Decryption

3. Exit

Enter your choice : 2

Enter Message to Decrypt:
K4qVJgSw3vwuRZnUD5YEzVHk41HP796bfHGz7iKNAt1MyLxjzsAUyE7p+5Ape5xo

Decrypted Message: Its KK29 aka Kaustubh

/**********MENU**********/

1. Encryption

2. Decryption

3. Exit

Enter your choice : 7

Wrong Choice,Please Choose Another Option.

/**********MENU**********/

1. Encryption

2. Decryption

3. Exit

Enter your choice : 3

Exit

Process finished with exit code 0

```
C:\Users\asus\PycharmProjects\AStar\Scripts\python.exe "C:/Users/asus/PycharmProjects/AStar/4. AES.py"
Enter Key: AISSMSIOIT
/*************MENU**************/
1. Encryption
2. Decryption
3. Exit
Enter your choice : 1
Enter Message to Encrypt: Its KK29 aka Kaustubh
Encrypted Message: K4qVJgSw3vwuRZnUD5YEzVHk41HP796bfHGz7iKNAt1MyLxjzsAUyE7p+5Ape5xo
/*************MENU**************/
1. Encryption
2. Decryption
3. Exit
Enter your choice : 2
Enter Message to Decrypt: K4qVJgSw3vwuRZnUD5YEzVHk41HP796bfHGz7iKNAt1MyLxjzsAUyE7p+5Ape5xo
Decrypted Message: Its KK29 aka Kaustubh
/*************MENU**************/
1. Encryption
2. Decryption
3. Exit
Enter your choice : 7
Wrong Choice,Please Choose Another Option.
/*************MENU**************/
1. Encryption
2. Decryption
3. Exit
Enter your choice : 3
Exit

Process finished with exit code 0
```