**Final Year B.Tech. (CSE) – VII [ 2024-25]**

**6CS451: Cryptography and Network Security Lab (C&NS Lab)**

**Date: 26/08/2024**

**Assignment 6**

**PRN:** 21510097  **Name: Viraj Patil**

1. **Apply AES algorithm for practical applications**

Ans:

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that is both fast and secure. It is the standard encryption algorithm used by governments, financial institutions, and many other organizations. Unlike DES, which is now considered insecure, AES is robust and provides a high level of security.

**Practical Application of AES Algorithm**

We can use the **pycryptodome** library in Python to implement AES encryption and decryption. The AES algorithm can work with key sizes of 128, 192, or 256 bits, and it operates on 128-bit blocks. In this example, we'll use AES with a 256-bit key in Cipher Block Chaining (CBC) mode.

**Python Code:**

from Crypto.Cipher import AES

from Crypto.Util.Padding import pad, unpad

from Crypto.Random import get\_random\_bytes

def aes\_encrypt(plain\_text, key):

    """

    Encrypt the plain text using AES algorithm.

    Parameters:

    plain\_text (str): The text to be encrypted.

    key (bytes): The encryption key (must be 16, 24, or 32 bytes long).

    Returns:

    bytes: The initialization vector (IV) and the encrypted cipher text.

    """

    cipher = AES.new(key, AES.MODE\_CBC)

    iv = cipher.iv  # Initialization vector

    padded\_text = pad(plain\_text.encode(), AES.block\_size)

    encrypted\_text = cipher.encrypt(padded\_text)

    return iv, encrypted\_text

def aes\_decrypt(iv, cipher\_text, key):

    """

    Decrypt the cipher text using AES algorithm.

    Parameters:

    iv (bytes): The initialization vector used during encryption.

    cipher\_text (bytes): The encrypted text to be decrypted.

    key (bytes): The decryption key (must be 16, 24, or 32 bytes long).

    Returns:

    str: The decrypted plain text.

    """

    cipher = AES.new(key, AES.MODE\_CBC, iv)

    decrypted\_text = unpad(cipher.decrypt(cipher\_text), AES.block\_size)

    return decrypted\_text.decode()

def main():

    """

    The main function to run the program.

    """

    print("\nAES Encryption and Decryption")

    # Generate a random 32-byte key for AES (256-bit)

    key = get\_random\_bytes(32)

    print(f"\nGenerated Key (in hexadecimal): {key.hex()}")

    # Input plaintext

    plain\_text = input("\nEnter the plain text to encrypt: ")

    # Encrypt the plaintext

    iv, encrypted\_text = aes\_encrypt(plain\_text, key)

    print(f"\nInitialization Vector (IV) (in hexadecimal): {iv.hex()}")

    print(f"\nEncrypted Text (in hexadecimal): {encrypted\_text.hex()}")

    # Decrypt the ciphertext

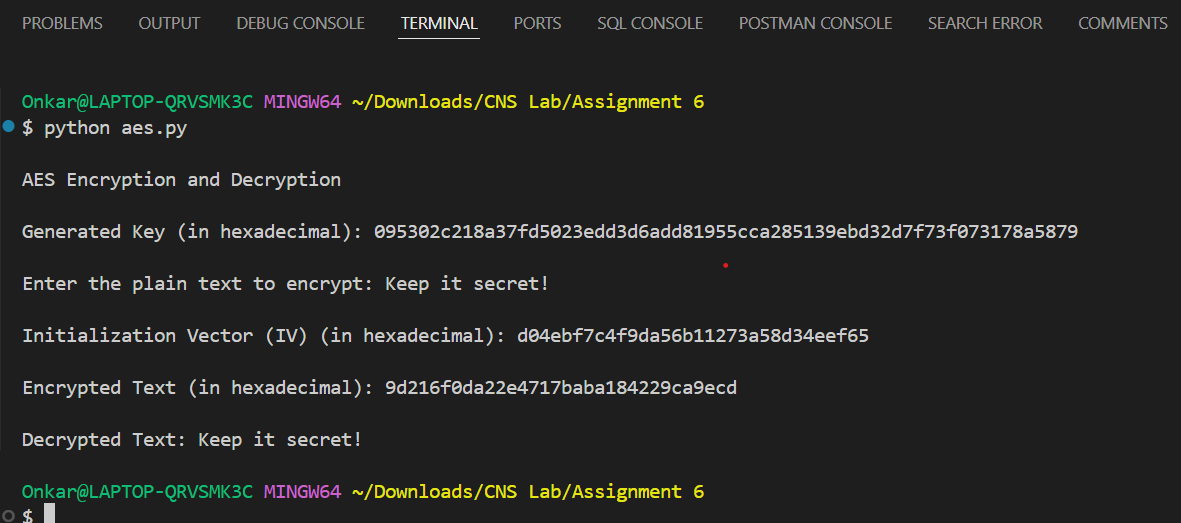
    decrypted\_text = aes\_decrypt(iv, encrypted\_text, key)

    print(f"\nDecrypted Text: {decrypted\_text}")

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

    main()

**Output:**



**Practical Applications of AES:**

* **File Encryption:** Encrypting sensitive files before storing them on disk.
* **Secure Communication:** Ensuring that data sent over the network remains confidential.
* **Data Protection in Applications:** Encrypting user data, such as passwords, to protect them from unauthorized access.

AES is widely adopted due to its strength and efficiency, and it remains the standard for securing digital data across various industries.