**Experiment 8**

**AIM:** Study and Use of Crypto++ Library to implement encryption and decryption

functions for different block ciphers

**Introduction:**

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data

established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely

used today as it is a much stronger than DES and triple DES despite being harder to implement.

**Points to remember:**

● AES is a block cipher.

● The key size can be 128/192/256 bits.

● Encrypts data in blocks of 128 bits each.

● That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output.

● AES relies on substitution-permutation network principle which means it is performed using a

series of linked operations which involves replacing and shuffling of the input data.

**Program:**

import pyaes

# A 256 bit (32 byte) key

key = "Smit\_1234567890\_Sutariya\_hello12"

plaintext = "Hello My name is not ViratKohli"

print("The plain text is:"+plaintext)

# key must be bytes, so we convert it

key = key.encode('utf-8')

aes = pyaes.AESModeOfOperationCTR(key)

ciphertext = aes.encrypt(plaintext)

# show the encrypted data

print("\nThe Encrypted text is:")

print(ciphertext)

# DECRYPTION

# CRT mode decryption requires a new instance be created

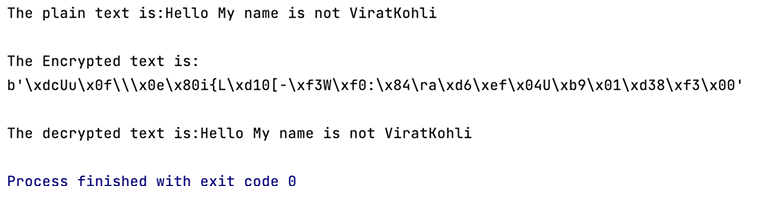
aes = pyaes.AESModeOfOperationCTR(key)

# decrypted data is always binary, need to decode to plaintext

decrypted = aes.decrypt(ciphertext).decode('utf-8')

print("\nThe decrypted text is:"+decrypted)

**Output:**

****

**Conclusion:**

After implementing the above Advance Encryption Standard algorithm is used for encryption and

decryption which is a much more efficient approach in comparison to other algorithms implemented

above.