**ADVANCED ENCRYPTION STANDARD (AES):**

-Mikhila CS22B1061

**CODE:**

from Crypto.Cipher import AES

from Crypto.Util.Padding import pad, unpad

from Crypto.Random import get\_random\_bytes

def encrypt(plaintext, key):

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

ciphertext = cipher.encrypt(pad(plaintext.encode(), AES.block\_size))

return cipher.iv + ciphertext

def decrypt(ciphertext, key):

iv = ciphertext[:16]

ciphertext = ciphertext[16:]

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

plaintext = unpad(cipher.decrypt(ciphertext), AES.block\_size)

return plaintext.decode()

plaintext = input("Enter the plaintext to encrypt: ")

key = get\_random\_bytes(16)

ciphertext = encrypt(plaintext, key)

print("\nEncrypted Ciphertext (hex):", ciphertext.hex())

decrypted\_text = decrypt(ciphertext, key)

print("\nDecrypted Text:", decrypted\_text)

**OUTPUT:**

Enter the plaintext to encrypt: assignment for network security

Encrypted Ciphertext (hex): bf7e925f97e5487c0e48168142b80e6b428a7818b81a238d5908241e924f4478ab58ff6c02bbb39ab5bfee5712dd5cb4

Decrypted Text: assignment for network security

**EXPLANATION OF THE IMPLEMENTATION:**

**Library Imports:**

Crypto.Cipher:

It provides AES encryption and decryption functionalities.

Crypto.Util.Padding:

This ensures plaintext is padded to fit the AES block size (16 bytes).

Crypto.Random:

This generates a random 128-bit key for encryption.

**Encryption Process:**

* Using the random key, a new AES cipher is created in CBC (Cipher Block Chaining) mode.
* Then, the plaintext is padded to be a multiple of 16 bytes.
* The ciphertext is generated and concatenated with the Initialization Vector.

**Decryption Process:**

* The IV (first 16 bytes) is extracted from the ciphertext.
* Then, the remaining bytes are decrypted using the same key and IV.
* Padding is removed to restore the original plaintext.

**Key Generation:**

* A 128-bit random key is generated using get\_random\_bytes(16).
* This key is required for both encryption and decryption.

**Output:**

The program displays the ciphertext in hexadecimal format. It then decrypts the ciphertext and prints the original plaintext.