Image Encryption and Decryption Using AES with Crypto++ Library

Objective:

Basic introduction to symmetric encryption using the AES (Advanced Encryption Standard) algorithm. You will be encrypting an image, and then decrypt it. Understand the basics of AES, key management, and how to apply these concepts to image files using the **Crypto++ library**.

What is AES?

- **Advanced Encryption Standard (AES)** is a widely used symmetric encryption algorithm. "Symmetric" means that the same key is used for both encryption and decryption.
- **AES** operates on blocks of data, typically 128 bits (16 bytes) at a time. The key size can vary (128, 192, or 256 bits), and the encryption process involves several rounds of transformation to ensure data security.

Key Terms:

- **Encryption**: The process of converting plain data (plaintext) into a coded format (ciphertext) that is unreadable without a specific key.
- **Decryption**: The process of converting ciphertext back into its original format using the corresponding key.
- **Symmetric Encryption**: An encryption method where the same key is used for both encryption and decryption.
- **Key**: A secret value used by the AES algorithm to encrypt and decrypt data. The security of the encrypted data relies on keeping this key secure.
- **Initial Vector (IV)**: A random value used alongside the key to enhance security by ensuring that the same plaintext encrypted multiple times will yield different ciphertexts. It does not need to be kept secret but must be unique for each encryption operation.
- **Crypto++ Library**: A C++ library that provides various cryptographic algorithms, including AES.

3. **Steps for Encryption Program**:
    - ○ Accept the image filename, key, and IV as inputs from the terminal.

○ **Use the Crypto++ library to encrypt the image using the AES algorithm.**
○ Save the encrypted image to a new file.

4. **Steps for Decryption Program**:

○ Accept the encrypted image filename, key, and IV as inputs from the terminal.
○ **Use the Crypto++ library to decrypt the image using the AES algorithm.** ○ Save the decrypted image to a new file and verify that it matches the original image.