TASK 6

1. Symmetric vs. Asymmetric Encryption

- **Symmetric (AES):** Uses a single shared key for both encryption and decryption. It is highly efficient for bulk data like files or disk encryption.
- **Asymmetric (RSA):** Uses a key pair—a Public Key for encryption and a Private Key for decryption. This is ideal for secure key exchange over public networks.

2. Data Integrity and Hashing Using **SHA-256**, I verified that any change to the input data results in a completely different hash value. This process is critical for ensuring that files or messages have not been modified during transmission.

3. Digital Signatures I successfully demonstrated that a digital signature (created with a private key) provides **non-repudiation**. This means the sender cannot deny sending the message, and the receiver can verify the sender's identity.

4. Real-World Applications

- **HTTPS:** Uses asymmetric encryption to safely exchange symmetric keys for a secure web session.
- **VPN:** Uses symmetric encryption (like AES) to protect data moving through a secure tunnel over the internet.