### Q2) Host a FTP and SFTP server , and try PUT and GET operations: FTP and SFTP Servers: Network Engineer's Perspective

**1. FTP (File Transfer Protocol) Server**

FTP is a standard network protocol used for transferring files between a client and a server over a TCP/IP network. It operates on **port 21** by default and uses a control channel for commands and a separate data channel for file transfers.

* **Modes:**
  1. **Active Mode:** The client opens a random high-numbered port and sends it to the server. The server connects back to this port for data transfer.
  2. **Passive Mode:** The server opens a random high-numbered port and informs the client. The client then initiates the data connection.

1. **Security Concerns:**
   1. Plaintext authentication (username/password)
   2. No encryption of data, vulnerable to packet sniffing
2. **Common Use Cases:**
   1. Legacy systems requiring fast, bulk file transfers
   2. Non-sensitive data exchange between internal networks

**2. SFTP (SSH File Transfer Protocol) Server**

SFTP is a secure alternative to FTP that operates over **SSH (port 22)**. Unlike FTP, it encrypts both commands and data, preventing eavesdropping.

* **Security Features:**
  + Uses SSH for authentication and encryption
  + Supports key-based authentication
  + No separate control and data channels (more firewall-friendly)
* **Common Use Cases:**
  + Secure file transfers over the internet
  + Remote server backup and automation
  + Environments with strict security policies

