SSH (Secure Shell)

SSH (Secure Shell) is **a cryptographic network protocol** used to securely access and manage remote machines over an unsecured network. It **provides strong encryption, authentication, and integrity** for communication between a client and a server, commonly used for remote login, file transfers, and tunneling.

Key Features of SSH

- **Secure Remote Access**: SSH allows users to remotely control a machine securely over a network, often used by system administrators and developers.
- **Encryption**: SSH uses encryption to protect data from being intercepted by attackers. This includes encrypting both the authentication process and the data transmitted during the session.
- **Authentication**: SSH supports password-based authentication as well as more secure methods like **public key authentication**, where the user's identity is verified using cryptographic keys.

Port 22

- **Port 22** is the default port used by SSH for communication. When a client initiates an SSH connection to a server, it usually connects through this port. However, for security reasons, some administrators choose to change the default SSH port to a non-standard port to avoid common brute force attacks.

SSH Handshake and Encryption

- **Asymmetric Encryption for Key Exchange**: During the initial handshake between the client and the server, SSH uses asymmetric encryption to exchange information securely. In asymmetric encryption, a public key and private key pair is used. The server sends its public key to the client, which encrypts data using this key. Only the server can decrypt this data with its private key.
- **Symmetric Key Generation**: Once the handshake is complete, the client and server agree on a symmetric key. Symmetric encryption is faster and more efficient than asymmetric encryption, so SSH uses it to encrypt the actual session data. The asymmetric encryption used in the handshake ensures that this symmetric key is exchanged securely.

SSH Handshake Process

1. **Client Request**: The client initiates a connection to the server (usually on port 22).
2. **Server Public Key**: The server sends its public key to the client.
3. **Key Exchange**: The client and server exchange cryptographic data using asymmetric encryption, which is then used to generate a shared symmetric key.
4. **Session Encryption**: Once the symmetric key is established, all subsequent communication is encrypted using this key, providing both confidentiality and integrity for the data.

Summary

- SSH is **a secure protocol** that allows remote management of systems using encryption.
- **Port 22** is the default communication port for SSH.
- The **SSH handshake starts with asymmetric encryption to securely exchange a symmetric key**, which is then used to encrypt the communication session for efficiency and speed.