**Week 3: Encryption, VPNs & Security Protocols**

**Objective:** Study encryption standards and secure communication protocols.

**Task#01: Explain the difference between symmetric and asymmetric encryption with examples.**

**Solution:**

**🔐 Symmetric Encryption**

**Definition:** Uses **one single key** for both encryption and decryption.

**How it works:**

* The sender encrypts the data using a secret key.
* The receiver uses the *same* key to decrypt it.
* Both parties must securely share the key beforehand.

**Example:**

* **AES (Advanced Encryption Standard)**
* **DES (Data Encryption Standard)**

**Use Case:**

* Encrypting files on disk
* Securing data in VPN tunnels (e.g., IPSec)

**Pros:**

* Fast and efficient for large data

**Cons:**

* Key distribution is risky—if someone intercepts the key, they can decrypt everything.

**🔑 Asymmetric Encryption**

**Definition:** Uses **two keys**: a **public key** to encrypt and a **private key** to decrypt.

**How it works:**

* The sender encrypts the message using the recipient’s **public key**.
* Only the recipient can decrypt it using their **private key**.

**Example:**

* **RSA (Rivest–Shamir–Adleman)**
* **ECC (Elliptic Curve Cryptography)**

**Use Case:**

* Secure email (e.g., PGP)
* SSL/TLS for HTTPS websites
* SSH authentication

**Pros:**

* No need to share private keys
* Great for secure communication over untrusted networks

**Cons:**

* Slower than symmetric encryption