Pre Lab:-

1.ECDSA Parameters Setup:

1. **Domain Parameter Generate:**
    - **Complex and public, often chosen from predefined published lists (e.g., curve parameters). These parameters define the elliptic curve and the finite field used in cryptographic operations.**
2. **Domain Parameter Validate:**
    - **Easy to validate and publicly available to ensure correctness. Validation ensures that all parameters conform to the required mathematical properties for security.**
3. **Key Pair Generate:**
    - **The private key is generated easily and kept secret, while the corresponding public key is derived from it. The private key is a random integer, and the public key is a point on the elliptic curve.**
4. **Key Pair Validate:**
    - **Public key validation is straightforward and ensures it lies on the selected elliptic curve. This step ensures that the key pair follows the curve's mathematical rules for correct and secure usage.**

2.ECDSA Generation & Verification:

- **ECDSA Signature Generation:**

  The signer uses their private key to generate a signature on a hashed message. This involves computing a random integer and solving an equation based on elliptic curve mathematics to produce two values, r and s, which together form the signature.

- **ECDSA Signature Verification:**

  The verifier uses the signer's public key and the signature (r and s) to check the authenticity of the message. The verifier ensures that the values satisfy the elliptic curve equation, confirming that the message was signed with the corresponding private key.

VIVA:-

1. **What is Key Pair Validate: Easy & public?**
   Key pair validation ensures that the public key lies on the elliptic curve, confirming it conforms to the cryptographic rules. This is a simple, publicly verifiable process.
2. **What is Key Pair Generate: Easy & private?**
   Key pair generation involves creating a random private key and deriving the corresponding public key through elliptic curve calculations. The private key remains secret, while the public key is shared.

3. **Explain use of ECC in Blockchain**
   ECC (Elliptic Curve Cryptography) is used in blockchain for generating secure public-private key pairs and digital signatures, ensuring secure transaction verification.

4. **Explain benefit of ECC in Blockchain**
   ECC provides strong security with smaller key sizes, which reduces storage and computational requirements, making it more efficient for blockchain systems.

5. **Describe working of digital signature using ECC**
   Digital signatures in ECC involve signing a hashed message with a private key, and the public key is used to verify the signature, ensuring message authenticity and integrity.