Pre-Lab:

1. Understand the Group, Ring, Field

- **Group**: A set combined with an operation that satisfies four conditions: closure, associativity, identity, and inversibility. Groups are foundational in abstract algebra and cryptography.
- **Ring**: A set equipped with two operations (commonly addition and multiplication) where the set is an abelian group under addition and is associative under multiplication. Rings also include a distributive property linking the two operations.
- **Field**: A ring where every non-zero element has a multiplicative inverse. Fields are crucial in algebra and are used in defining finite fields for cryptography.

2. Understand Why We Need Elliptic Curve Cryptography (ECC)

- **ECC**: ECC is a type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. It provides the same level of security as traditional systems like RSA but with much smaller key sizes, leading to faster computations and reduced storage requirements.

3. Understand the Elliptic Curve Schemes

- **Elliptic Curve Digital Signature Algorithm (ECDSA)**: A cryptographic algorithm used to ensure the authenticity and integrity of a message or document. ECDSA is widely used in digital signatures.
- **Elliptic Curve Pintsov Vanstone Signature (ECPVS)**: A variant of ECDSA designed for specific applications like message recovery. It allows partial message recovery from the signature.
- **Elliptic Curve Diffie-Hellman (ECDH)**: A key exchange protocol allowing two parties to establish a shared secret over an insecure channel using elliptic curves. ECDH is essential for secure communications.

VIVA:

1. Why We Need Elliptic Curve Cryptography (ECC)

ECC provides strong security with smaller key sizes, leading to faster computations and lower resource usage compared to traditional algorithms like RSA.

2. Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA is a cryptographic algorithm used for creating digital signatures that ensure the authenticity and integrity of messages.

3. What Is the Advantage of ECC

ECC offers the same level of security as traditional methods with significantly smaller key sizes, making it more efficient in terms of speed and resource usage.

4. What Is the Advantage of Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA provides strong security for digital signatures while requiring less computational power and storage space, making it ideal for modern applications.

5. How ECDSA Is Helpful in Blockchain

ECDSA secures blockchain transactions by ensuring that only the rightful owner of a private key can authorize a transaction, thus protecting the integrity of the blockchain.