PostLab:-

1. Advantages of Elliptic Curve Cryptography (ECC)

- **Stronger Security with Smaller Keys:** ECC provides strong encryption with much smaller key sizes compared to RSA. For example, a 256-bit ECC key offers similar security to a 3072-bit RSA key.
- **Faster Computations:** ECC requires less computational power, making it faster for encryption, decryption, and key generation.
- **Reduced Storage and Bandwidth:** Smaller key sizes reduce storage requirements and bandwidth usage, making ECC ideal for environments with limited resources, like mobile devices.

Disadvantages of Elliptic Curve Cryptography (ECC)

- **Complex Implementation:** ECC algorithms are more complex to implement correctly compared to RSA, leading to a higher chance of security flaws if not implemented properly.
- **Patent Issues:** Some ECC algorithms have been subject to patents, which can limit their use or increase costs.
- **Limited Adoption:** While ECC is becoming more popular, it still isn't as widely adopted as RSA, which may cause compatibility issues.

2. Applications of Elliptic Curve Cryptography (ECC)

- **Secure Communication:** ECC is used in SSL/TLS certificates to secure web traffic (HTTPS).
- **Mobile Devices:** ECC's efficiency makes it ideal for use in smartphones and IoT devices where processing power and battery life are limited.
- **Cryptocurrencies:** ECC is widely used in blockchain technology and cryptocurrencies, such as Bitcoin, for secure key generation and digital signatures.
- **Digital Signatures:** ECC is used in digital signature algorithms (like ECDSA) for verifying the authenticity of messages and documents.