Pre Lab:-

1. Secure Hash Algorithm (SHA-1)

SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) in 1993. It's part of the SHA family of algorithms, which produce fixed-length hash values from input data. SHA-1 generates a 160-bit (20-byte) hash value, often referred to as a "message digest."

Properties of SHA-1:

- **Deterministic**: The same input will always produce the same hash.
- **Fixed Output Size**: SHA-1 produces a 160-bit hash value, regardless of the input size.
- **Infeasible to invert**: Given a hash value, it's computationally infeasible to retrieve the original input.
- **Collision Resistance**: It should be hard to find two different inputs that result in the same hash. However, SHA-1 has been deprecated due to vulnerabilities in its collision resistance, as researchers have discovered weaknesses allowing attackers to find collisions in feasible time.

2. Digital Signature Standard (DSS) and Its Use of SHA-1

The **Digital Signature Standard (DSS)** is a federal standard for digital signatures, issued by NIST in 1991. The **Digital Signature Algorithm (DSA)** is part of the DSS and is used to generate and verify digital signatures. DSS relies on the SHA-1 algorithm to ensure message integrity.

How DSS Uses SHA-1:

- **Message Hashing**: Before a digital signature is applied, DSS uses the SHA-1 algorithm to generate a hash (digest) of the message. This digest serves as a fixed-length representation of the message content.
- **Signature Generation**: Once the SHA-1 hash of the message is generated, DSS signs this hash using DSA and a private key. This ensures that the signature is compact and does not reveal the entire message.
- **Signature Verification**: When verifying a signature, DSS recalculates the SHA-1 hash of the original message and checks if the corresponding signature, when decrypted with the public key, matches the recalculated hash.

VIVA:-

1. **What is Secure Hash Algorithm (SHA)-1?**
   SHA-1 is a cryptographic hash function that produces a 160-bit hash value from any input, used primarily for data integrity verification. It has been deprecated due to weaknesses in its collision resistance.
2. **What is Digital Signature Standard (DSS) and how does it use the SHA hash algorithm?**
   DSS is a standard for digital signatures, using SHA-1 to hash a message before applying a digital signature through the Digital Signature Algorithm (DSA).

3. **What is the advantage of a hashing algorithm?**
   Hashing ensures data integrity by creating a fixed-size digest of the input, making it efficient for detecting alterations in data.

4. **How can a hashing algorithm be used in blockchain?**
   Hashing secures blockchain transactions by linking blocks with hash values, ensuring tamper-proof data integrity and enabling proof of work.

5. **What is the difference between hashing and encryption?**
   Hashing generates a fixed-length representation of data for integrity checks and is one-way, while encryption encodes data to be reversible by authorized users.