SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107 An Autonomous Institution Accredited by NBA – AICTE and Accredited by NAAC
UGC wit'A' Grade Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING IOT Including CS&BCT
COURSE NAME : DISTRIBUTED LEDGER TECHNOLOGY

TOPIC: Introduction to Digital Signatures

Introduction to Digital Signatures

A digital signature is a cryptographic technique used to authenticate the identity of the sender and ensure the integrity of the message or document. It acts as a virtual equivalent to a handwritten signature, but with much stronger security. Digital signatures are created using a pair of keys: a private key for signing the data, and a public key for verifying the signature. This ensures that the data has not been altered and that the sender is authentic. The process is designed to guarantee non-repudiation, meaning the sender cannot deny having signed the document.

How Digital Signatures Work

Digital signatures rely on asymmetric cryptography to function. The process begins with the document or message being hashed, meaning a fixed-size output (a hash) is created from the original content. Then, the private key of the sender is used to encrypt this hash, forming the digital signature. When the recipient gets the document, they use the public key to decrypt the signature and verify the hash. If the decrypted hash matches the hash of the received document, it confirms that the document is intact and comes from the expected sender.

Applications of Digital Signatures

Digital signatures are widely used in various industries to ensure the security and authenticity of documents and transactions. Some common applications include:

- E-commerce: Verifying online transactions and digital contracts.
- Email Authentication: Ensuring the email was sent by the claimed sender and has not been tampered with.
- Software Distribution: Ensuring software is authentic and has not been altered by malicious parties.
- Legal Documents: Providing an electronic, legally binding signature for contracts, agreements, and other official documents.

Advantages and Limitations of Digital Signatures

Digital signatures offer several important advantages:

- They provide authenticity, ensuring that the signature is linked to the signer and the document.
- They ensure integrity, meaning the document has not been altered since it was signed.
- They offer security, reducing the risk of fraud, as the signature cannot easily be forged. However, there are some limitations:
- Digital signatures require careful private key management. If the private key is lost or stolen, the signer's identity could be compromised.
- The Public Key Infrastructure (PKI) used to manage keys must be well-managed. If the PKI fails, the security of the entire system could be at risk.