Dr.SNS RAJALAKSHMI COLLEGE OF ARTS AND SCIENCE
(Autonomous)

Accredited by NAAC – UGC with 'A+ Grade (Cycle IV)

(Recognized by UGC, Approved by AICTE & Affiliated to Bharathiar University)

Coimbatore- 49

DEPARTMENT OF COMMERCE WITH INFORMATION TECHNOLOGY

21UCI505 – BLOCKCHAIN AND DISTRIBUTIVE LEDGER

Unit-2: Basic Crypto Primitives: Hash and Digital Signature

Ms. S.Meenakshi, Assistant Professor

Department of Commerce with Information Technology

Basic Crypto Primitives: Hash and Digital Signature

1. Cryptographic Hash Function (Hash)

A hash function is a mathematical algorithm that converts input data of any size into a fixed-length output called a *hash value* or *digest*.

Key Characteristics

Deterministic: Same input → same hash every time

Fixed length: Output length is constant (e.g., SHA-256 → 256 bits)

One-way: Cannot reverse the hash to get original data

Collision resistant: Very hard to find two inputs with the same hash

Avalanche effect: Small change in input → drastic change in hash

USES

- Data integrity verification
- Password storage (with salt)
- Blockchain block linking
- Digital fingerprints of files

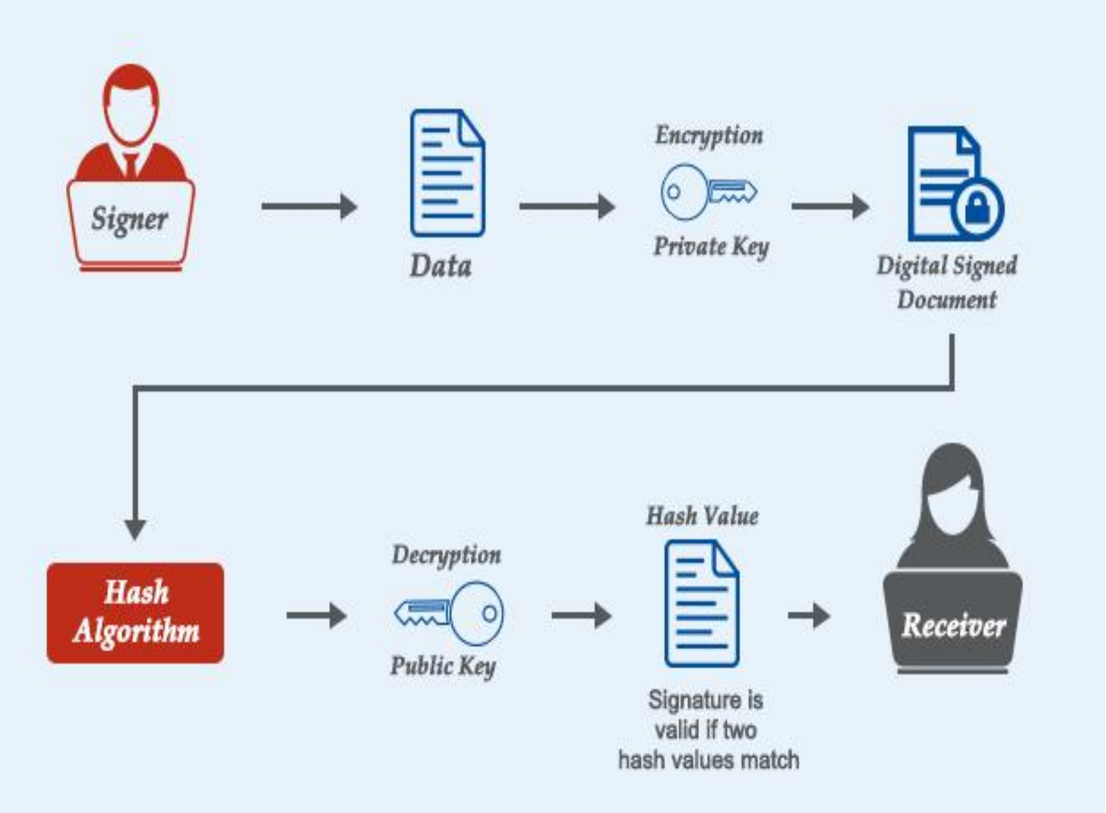
2. Digital Signature

A digital signature ensures authentication, integrity, and non-repudiation using asymmetric cryptography.

Key Components

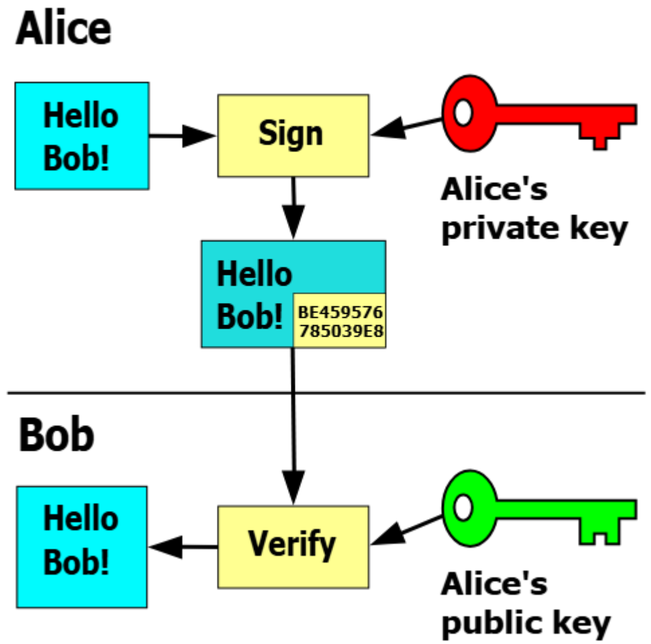
Private Key: Used to create the signature (kept secret)

Public Key: Used to verify the signature (shared openly)



How It Works

- Sender hashes the message
- Hash is encrypted using sender's **private key** → digital signature
- Receiver decrypts using sender's **public key**
- If hashes match → message is authentic and unchanged



Hash vs Digital Signature (Quick Comparison)

Aspect	Hash	Digital Signature
Purpose	Integrity	Integrity + Authentication
Keys Required	No	Yes (Public & Private)
Reversible	No	Verification possible
Blockchain Use	Block linking	Transaction validation

THANK YOU