THE CRYPTO BRIDGE

THE FOSS FILES | SEASON 5 | EPISODE 3

THE CIPHER FILES

Sharvari Jadhav

Sandesh Shinde

Aditya Aparadh

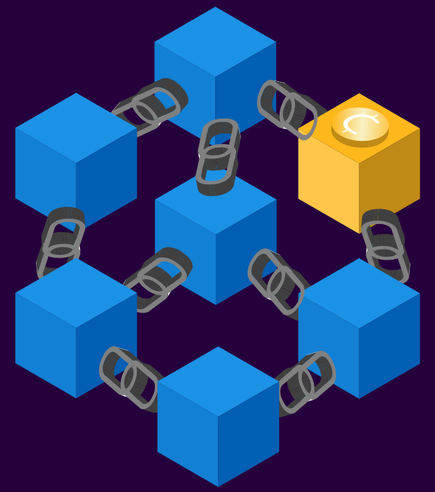
WLUG
COMMUNITY | KNOWLEDGE | SHARE

TABLE OF CONTENT

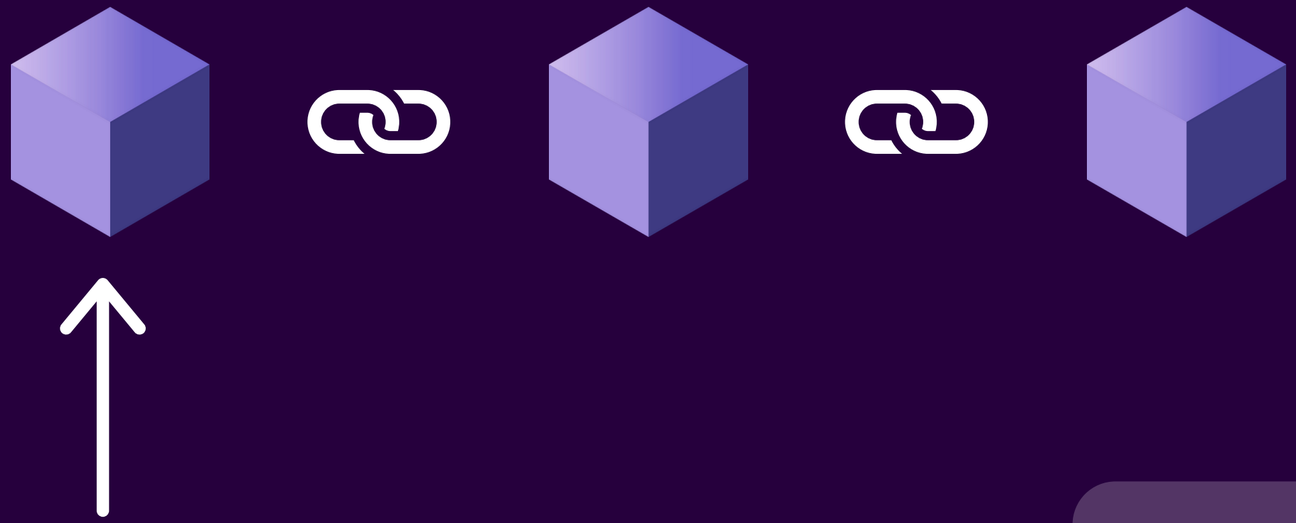
WLUG
COMMUNITY | KNOWLEDGE | SHARE

BLOCKCHAIN

- Blockchain technology is a type of distributed ledger technology (DLT)
- It is an accounting system where the ledger (record of transactions) is distributed among a network of computers



BLOCKCHAIN



Single block = Single record

Record

Relevent Information (Transaction)

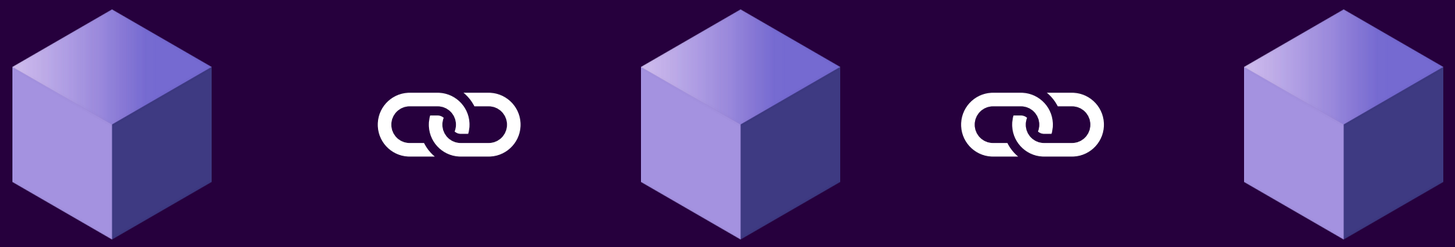
A unique cryptographic hash

The hash of the previous block

WLUG
COMMUNITY | KNOWLEDGE | SHARE

HOW IT WORKS?

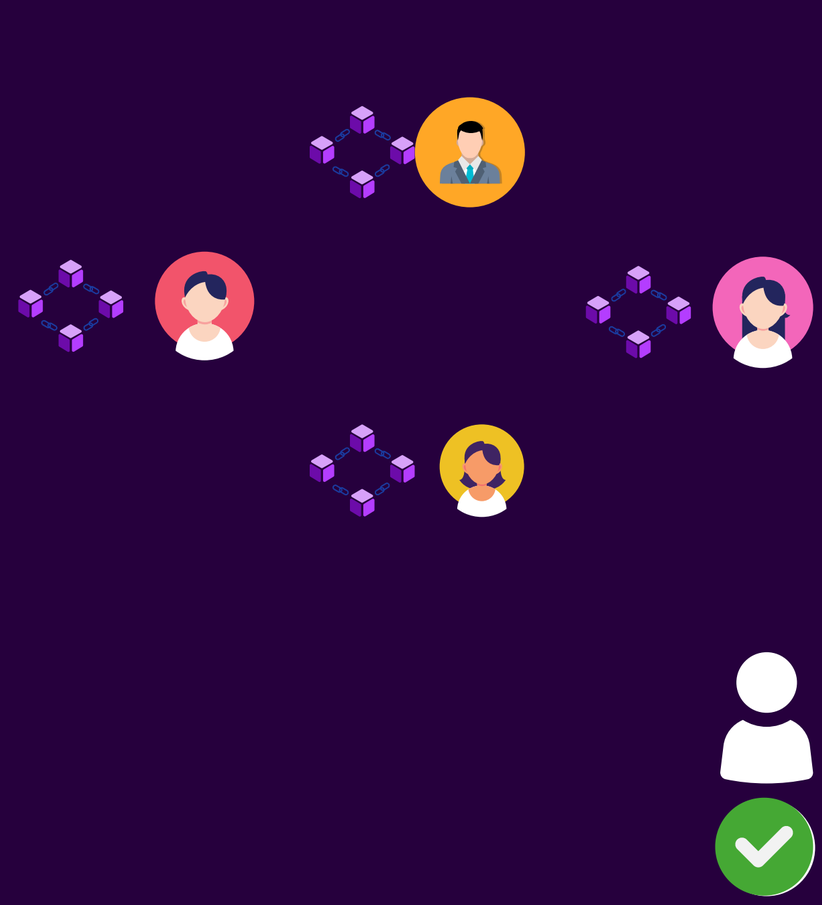
Genisis Block



Hash: **AAAA**	Hash: **BBBB**	Hash: **CCCC**
Prev Hash: **0000**	Prev Hash: **AAAA**	Prev Hash: **BBBB**

CONSENSUS MECHANISM

Proof of Work (PoW)



PUBLIC AND PRIVATE KEY

WLUG
COMMUNITY | KNOWLEDGE | SHARE

APPLICATIONS

- Cryptocurrencies
- Voting Systems
- Smart Contracts
- DeFi (Decentralized Finance)
- Supply Chain Management
- Healthcare Records

PRETTY GOOD PRIVACY(PGP)

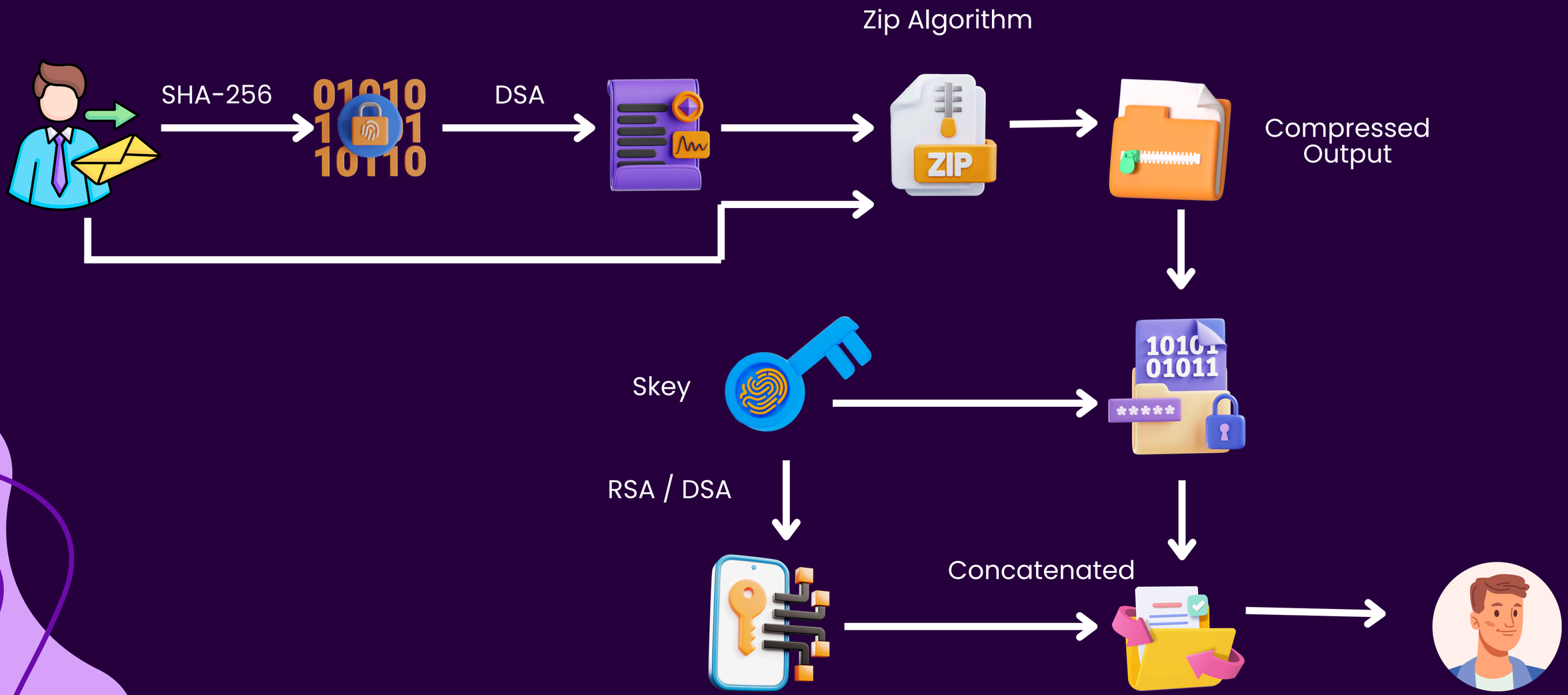
PGP is an information’s encryption technology
It provides a framework to exchange data securely among peers

- **Symmetric encryption:** encrypts your data fast
- **Asymmetric encryption:** exchanges keys securely.
- **Digital signatures:** verify authenticity

TECHNIQUES USED

- Hybrid Cryptography (Symmetric + Asymmetric).
- Digital Signatures
- Hash Functions (e.g., SHA-1, SHA-256).
- Web of Trust
- Data Compression

HOW PGP WORKS?



GNU PRIVACY GUARD

GPG is the free implementation for PGP, while the original one is protected.

- Git Commits & Tag Signing
- Package Manager Security
- Encrypted Messaging
- Verifying Software Downloads
- Docker Image Signing
- Signing PDFs or Documents

WLUG
COMMUNITY | KNOWLEDGE | SHARE

PUBLIC KEY INFRASTRUCTURE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Session Key

Encrypted
data

Browser

Server

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Encrypt
Session Key

Browser

Server Public Key

Server

Encrypt
Session Key

Browser

Encrypted
Session Key

Server

Decrypted
Session Key

WLUG
COMMUNITY | KNOWLEDGE | SHARE

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Wait!!
What if ?

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Session Key

Browser

Encrypted data

Server

I am watching you

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Encrypt
Session Key

Browser

MITM
Public Key

Server
Public Key

Server

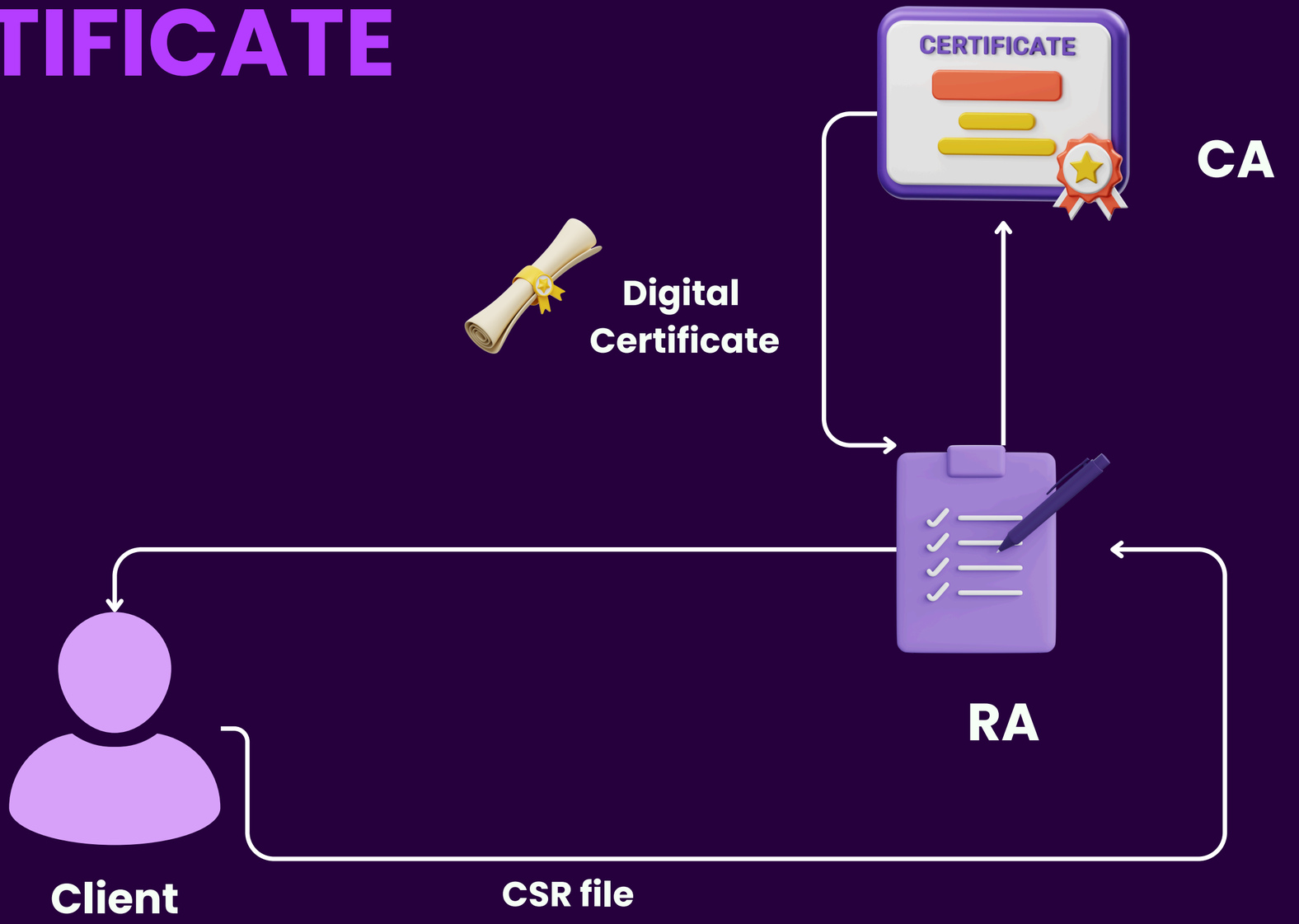
PUBLIC KEY INFRASTRUCTURE

- It is framework used to create, manage, distrubute, use, strore and revoke digital certificates
- PKI ensures :
  - confidentiality
  - integrity
  - authenticity
  - non-repudiation

PKI : COMPONENTS

- Certificate Authority (CA)
- Registration Authority (RA)
- Digital Certificates
- Public and Private Keys

ISSUING A DIGITAL CERTIFICATE



CSR : CERTIFICATE SIGNING REQUEST

- A Certificate Signing Request (CSR) is a standardized file used to request a digital certificate from a Certificate Authority (CA)
- Standard X.509
- Encoded in PEM format (Base64-encoded)

FIELDS IN A CSR

- Common Name (CN)
- Organization (O)
- Locality (L)
- State or Province (ST)
- Country (C)
- Public Key
- Signature Algorithm
- Email Address (optional)
- Subject Alternative Name (SAN) (optional)
- Version

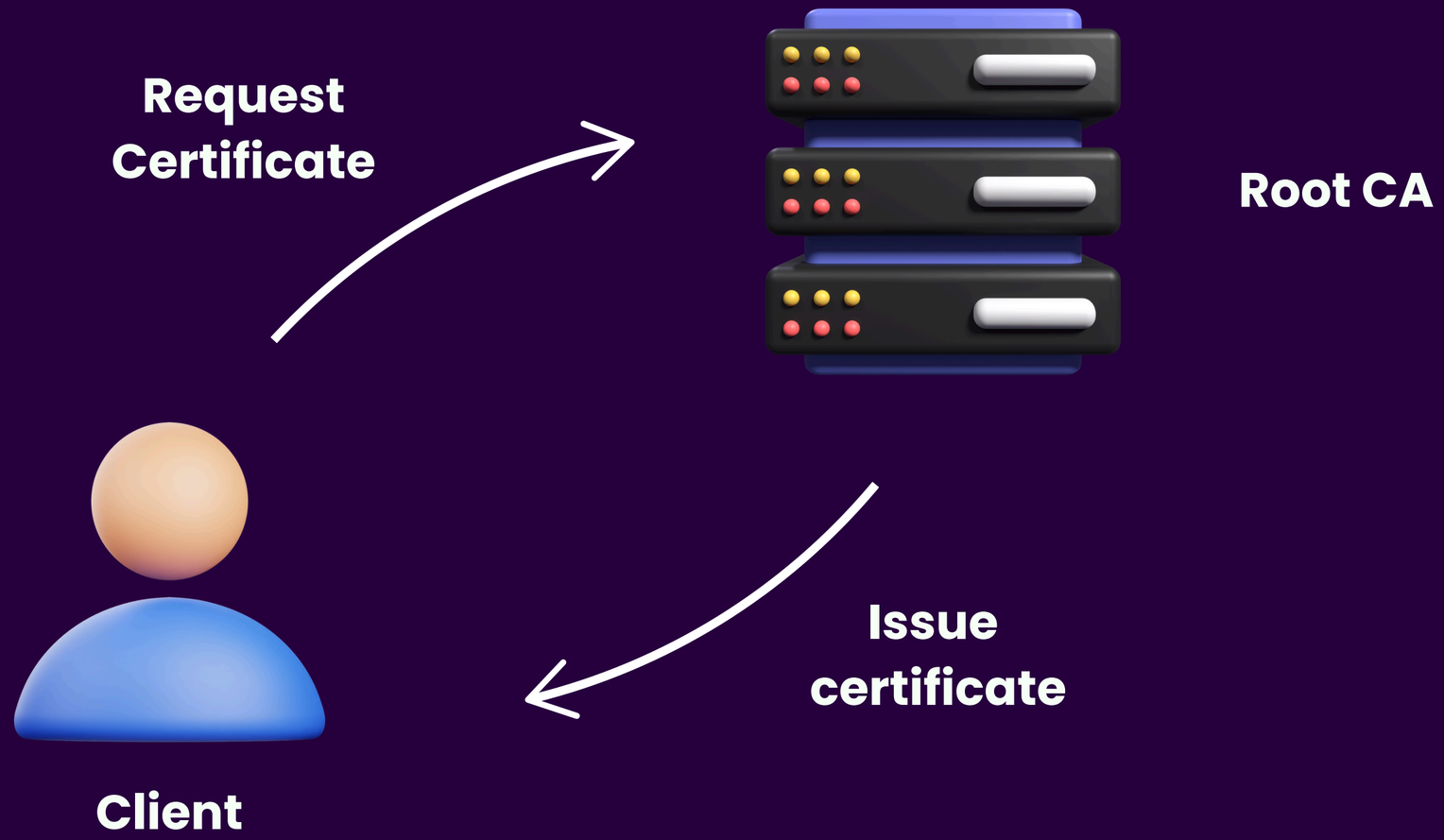
REGISTRATION AUTHORITY

- It acts as an intermediary between the Certificate Authority (CA) and the entity requesting a digital certificate
- Roles of CA :
    - Identity Verification
    - Forwarding Requests to the CA
    - Approving or Rejecting Certificate Requests
    - Certificate Revocation Requests

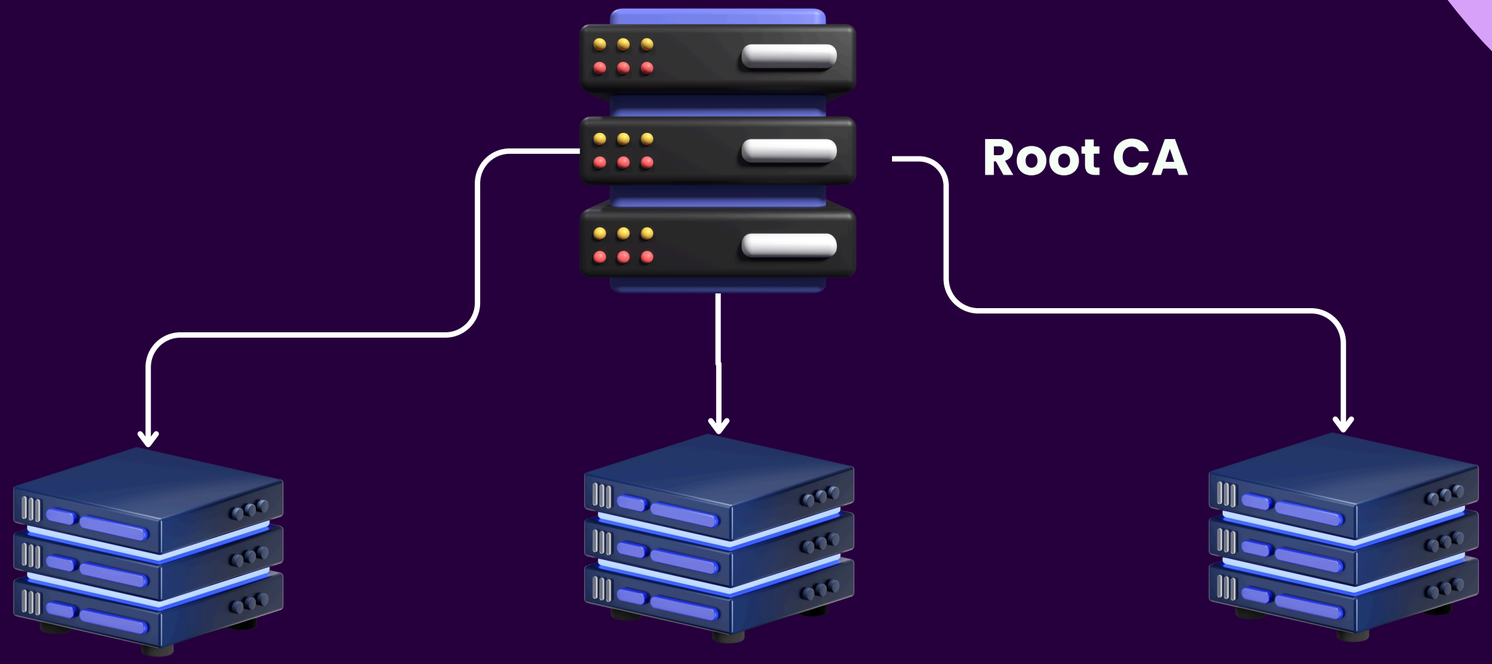
CERTIFICATE AUTHORITY

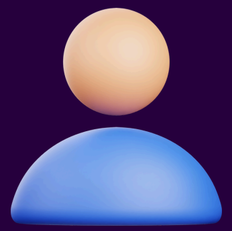
- A Certificate Authority (CA) is a trusted organization or entity responsible for issuing and managing digital certificates
- Roles of CA :
    - Issuing Digital Certificates
    - Establishing Trust
    - Certificate Revocation

CERTIFICATE AUTHORITY



CERTIFICATE AUTHORITY





Client

DIGITAL CERTIFICATE

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Validity Period
- Subject - DN,ON
- Public Key
- Signature Value

SIGNATURE VALUE

Digital Certificate

Hash Value

CA’s Private Key

Signature Value

WLUG
COMMUNITY | KNOWLEDGE | SHARE

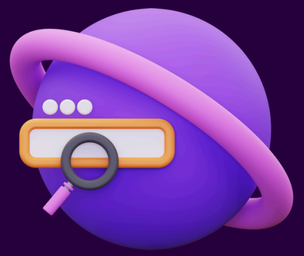
Public Key

Private Key

Session Key

Certificate Authority

CA's public key



Browser

Encrypted data

Server

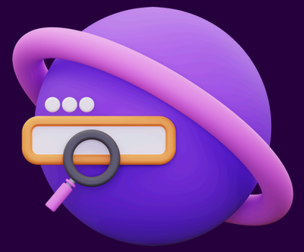
WLUG
COMMUNITY | KNOWLEDGE | SHARE

Public Key

Private Key

Session Key

Certificate Authority



Browser

Digital Certificate

Server

CA's public key

WLUG
COMMUNITY | KNOWLEDGE | SHARE

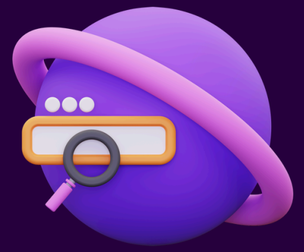
Public Key

Private Key

Session Key

Certificate Authority

CA's public key



Browser

Encrypted Session key

Server

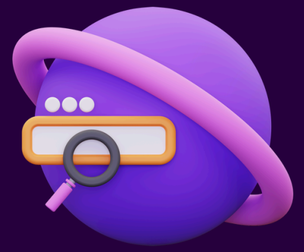
WLUG
COMMUNITY | KNOWLEDGE | SHARE

Public Key

Private Key

Session Key

Certificate Authority



Browser

Encrypted Data

Server

CA's public key

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Oh no, not again!

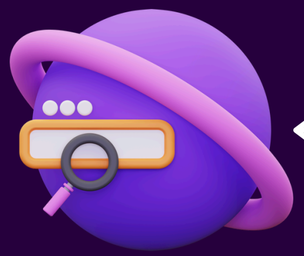
MITM

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Public Key

Private Key

Session Key



Browser

CA's public key

Modified Cert

OG Cert

Server

CA's public key

Scenario-1

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Digital Certificate

Server public key

Signature value(hash value)

Digital Certificate (modified)

Attacker public key

Signature value(hash value)

(modified)

Browser

Digital Certificate (modified)

Attacker public key

Signature value(hash value)

Hash of Modified Digital Certificate

Scenario-2

WLUG
COMMUNITY | KNOWLEDGE | SHARE

Digital Certificate

Server public key

Signature value(hash value)

CA's public key

Digital Certificate (modified)

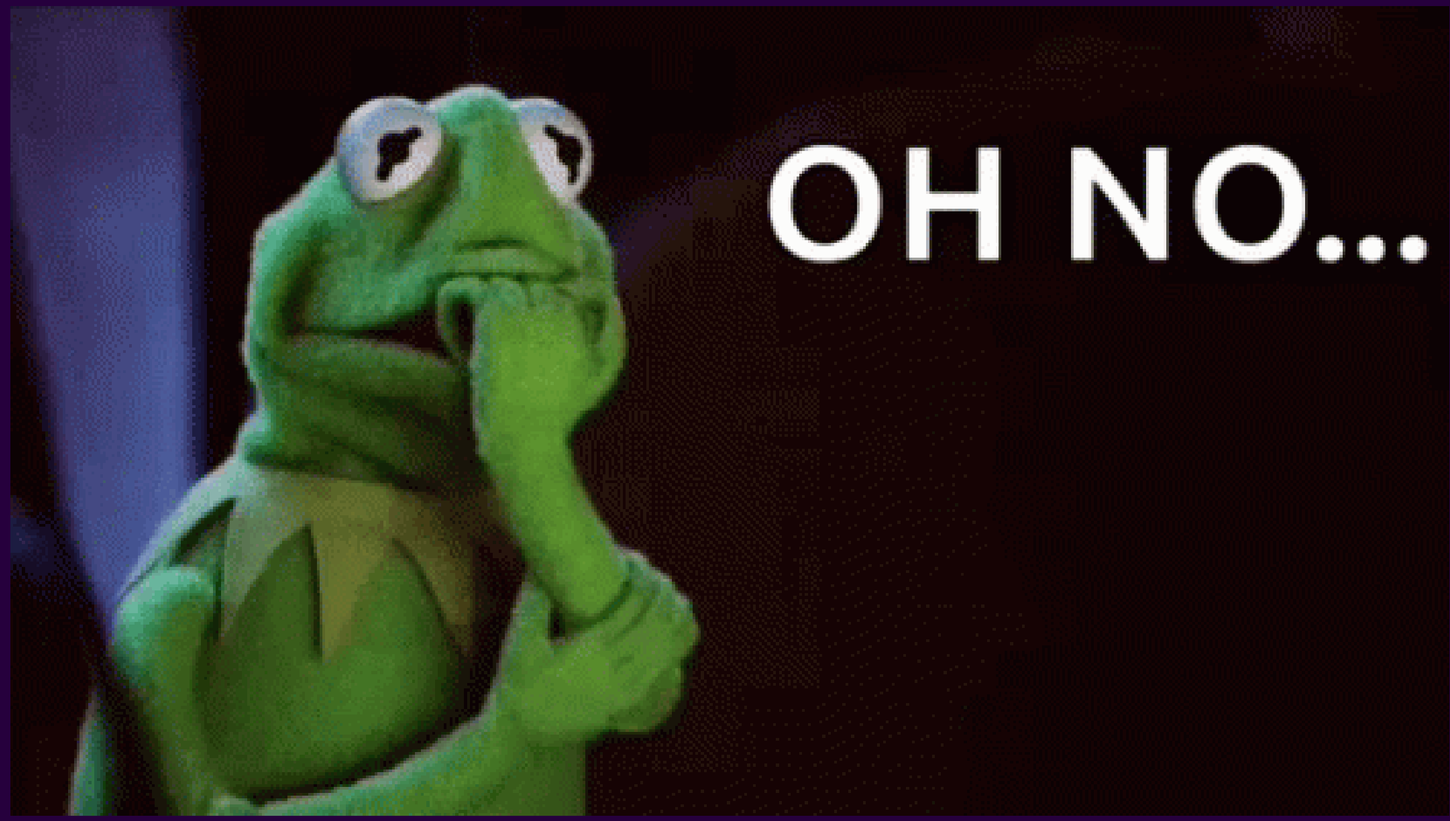
Attacker public key ←(modified)

Modify hash value ←(modified)

But hacker doesn't have private key of CA to encrypt hash value again

WLUG
COMMUNITY | KNOWLEDGE | SHARE

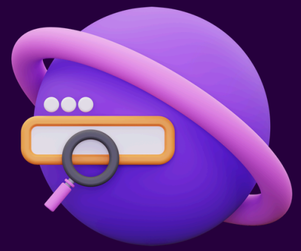
MITM Be Like!!



WLUG
COMMUNITY | KNOWLEDGE | SHARE

SECURE SOCKET LAYER

HTTP

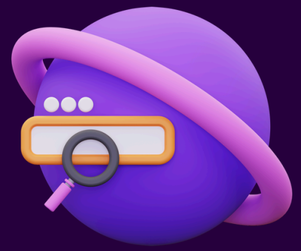


Browser

Data (PlainText)

Server

HTTPS



Browser

Data (Encrypted)

Server

WHAT IS SSL?

- SSL (Secure Sockets Layer) is a cryptographic protocol that provides security for communication over a network by using encryption to protect data transmitted between a client and a server.
- It ensures secure communication over the internet
- Features :
    - Encryption
    - Authentication
    - Data Integrity

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSL HANDSHAKE

SSL HANDSHAKE

1. Client Hello
2. Server Hello
3. Certificate
4. Server Hello Done
5. Client Key Exchange
6. Change Cipher Spec
7. Finished
8. Change Cipher Spec(Server)
9. Finished(Server)
10. Application Data

WLUG
COMMUNITY | KNOWLEDGE | SHARE

SSL

APPLICATIONS

HTTPS

Secure Mail

VPN

File Transfer

API Connections

Payment Gateways

THANK YOU