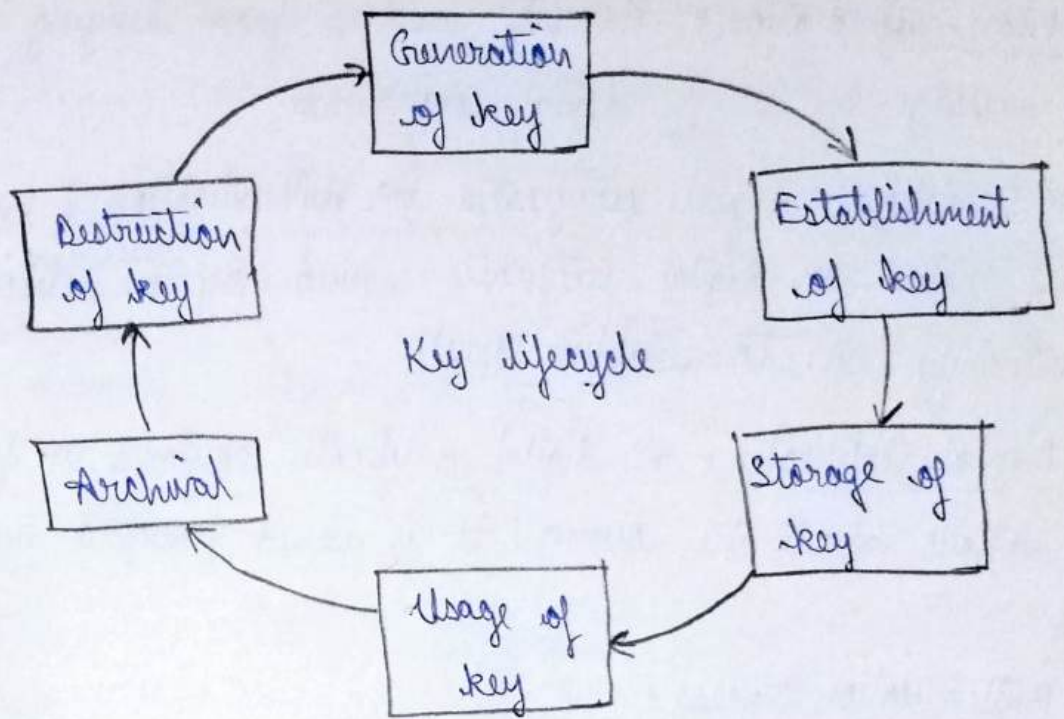


① Define Public Key Infrastructure (PKI) & explain its role in ensuring securing communication on the internet. How does PKI utilize digital certificates for authentication & encryption?

Ans Public Key Infrastructure (PKI) is the governing body behind issuing digital certificates. It helps to protect confidential data & gives unique identities to users & systems. Thus, it ensures security in communications. The public key infrastructure uses a pair of keys: the public key & the private key to achieve security. The public keys are prone to attacks & thus an intact infrastructure is needed to maintain them.

Managing keys in the Crypto System

- The security of a cryptosystem relies on its keys. Thus, it is important that we have a solid key management system in place.
- It involves managing the key life cycle which is as follows:-



Public Key Infrastructure affirms the usage of a public key. PKI identifies a public key along with its purpose. It usually consists of the following components:-

- A digital certificate also called a public key certificate
- Private key token
- Registration authority
- Certification authority
- CMS or Certification Management System

Role of PKI in Secure Communication

- ① Authentication Confirms the identity of individuals, websites and organizations
- ② Encryption Protects sensitive data by encoding it so that only the intended recipient can read it.
- ③ Data Integrity Ensures that transmitted data remains unchanged & has not ~~has~~ been tampered with.



④ Non-repudiation - Prevents senders from denying they sent a message by using digital signatures  
PKI utilizes digital certificates for Authentication & Encryption  
PKI relies on digital certificates issued by a Certificate Authority (CA) to establish trust.

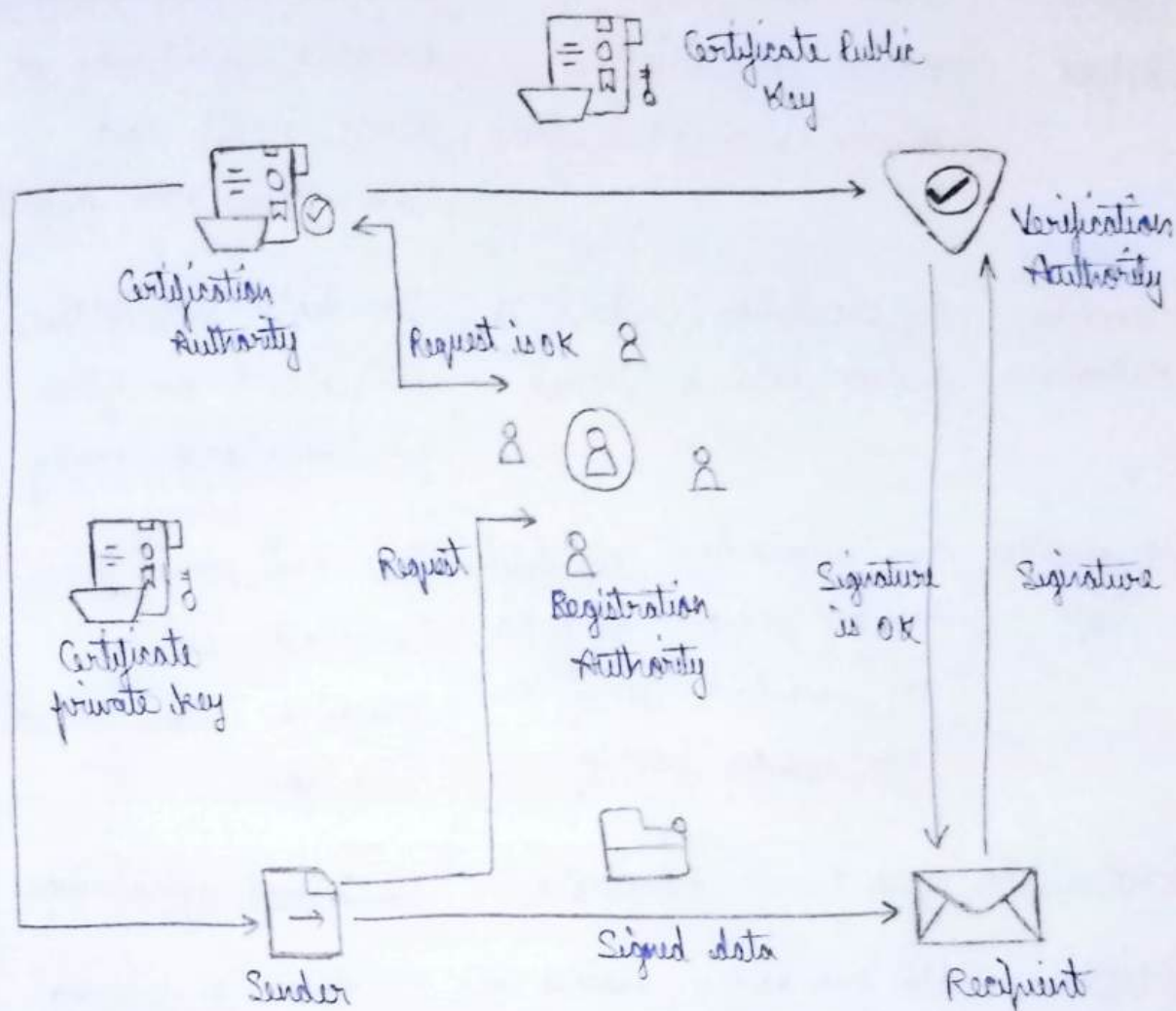
① Digital Certificates - A digital certificate contains a public key & details about the owner. It is issued & signed by a trusted CA

② Authentication Process -

- When a client (browser) connects to a website, it receives the server's digital certificate.
- The client verifies the Certificate's Authenticity by checking the CA's signature & certificate validity.
- If valid, the client trusts the server's identity.

③ Encryption Process

- PKI uses asymmetric encryption to establish a secure session
- The client encrypts a secret key using the server's public key from the certificate
- Only the server can decrypt the secret key using its private key, establishing a secure encrypted channel.



② Compare and contrast secure socket layer (SSL) and secure electronic transaction (SET) protocols in terms of their

Ans - SSL & SET are both security protocols designed to secure online transactions, but they serve different purposes & have distinct security mechanisms.

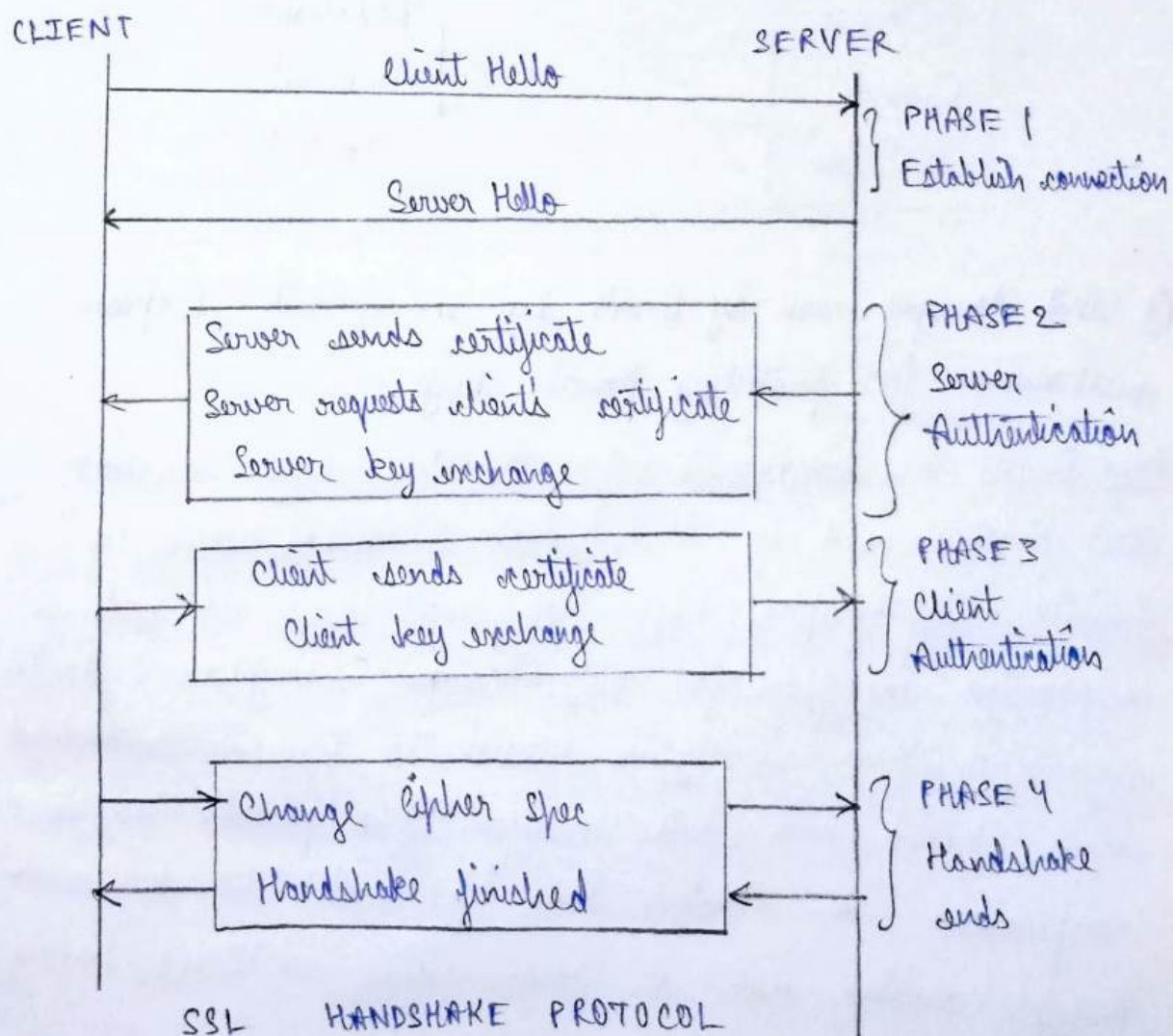


Feature	Secure Socket Layer (SSL)	Secure Electronic Transaction (SET)
① Purpose	Secures communication between a client & server	Designed specifically for secure credit card transactions over internet
② Security Mechanisms	Uses encryption (SSL/TLS) to protect data in transit	Uses digital signatures, certificates & encryption for transactional security
③ Encryption Type	Uses asymmetric encryption for key exchange followed by symmetric encryption for session security.	Uses dual encryption (merchant sends transaction details but not card details)
④ Authentication	Uses server authentication	Uses mutual authentication
⑤ Digital Signatures	Not mandatory, mainly used in SSL Certificates for website authentication	Mandatory for ensuring the integrity & authenticity of transactions
⑥ Certificate Authority (CA)	Certificates are issued to servers & sometimes clients	Involves multiple CAs for banks, merchants & customers
⑦ Ease of Implementation	Widely supported, easy to implement	Complex setup requiring special infrastructure & agreements between bank, merchants & users
⑧ Use Case	General purpose secure communication (HTTPS, VPNs, emails, etc)	Used exclusively for <del>the</del> online credit card transactions

## Suitability for online transactions

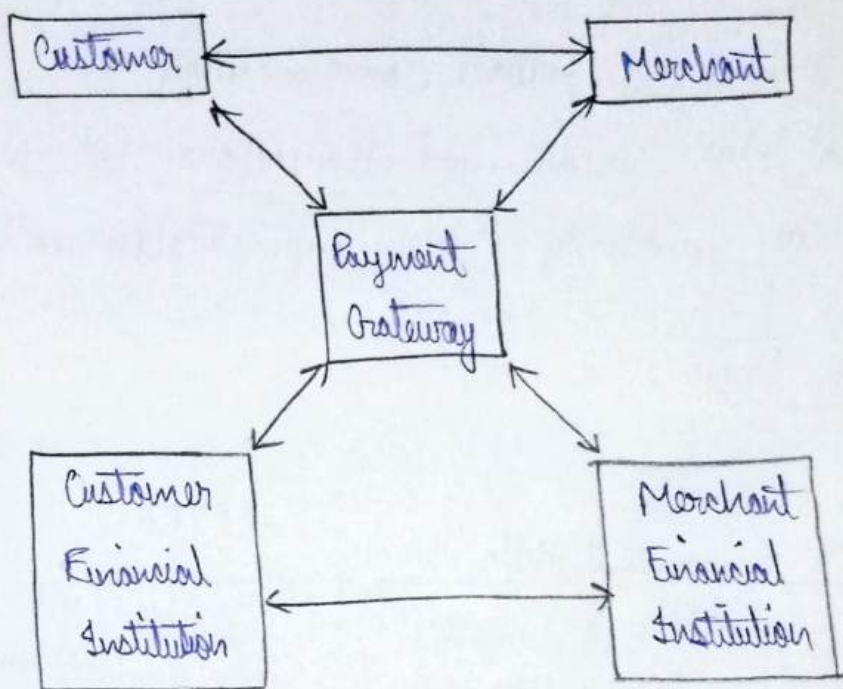
- SSL is suitable for general web security including e-commerce, banking & private communication
- SET is ideal for credit card transactions but is rarely used due to its complexity & high implementation costs

## Secure Socket Layer





## Secure Electronic Transaction (SET) :



③ What do you mean by Private key management? Explain mechanisms for protecting private keys.

Ans: Private key management refers to the process, technologies, best practices used to store, protect & control access to private cryptographic keys. Since private keys are used in asymmetric encryption for authentication, encryption & digital signatures, their security is crucial to prevent unauthorized access, fraud and data breaches. If a private key is compromised, an attacker can impersonate the key owner, decrypt sensitive data or forge digital signatures, leading to serious security risks.

# Mechanisms for Protecting Private Keys:

## (i) Hardware Security Modules (HSMs):

- Dedicated hardware devices designed to securely generate, store and manage private keys.
- Prevents key extraction & provides tamper-proof security
- Commonly used in banks, enterprise and cloud services

## (ii) Secure Key Storage (Software & Hardware):

- Protects keys in Trusted Platform Modules (TPMs), secure enclaves and encrypted software storage (AES-256)
- Prevents direct access to private keys, reducing risks of theft or leakage.

## (iii) Multi Factor Authorization (MFA) for Key Access:

- Requires multiple authentication methods (password + biometrics) to access private keys
- Even if a password is compromised, attackers cannot ~~connect~~ access the key without additional verification
- Used in cryptographic wallets, cloud key management systems & enterprise security.

## (iv) Key Rotation & Expiry Policies:

- Regularly updates and replaces private keys to minimize the risks associated with compromised keys.
- If a key is exposed, its validity is limited to a short period.



→ Ex:- SSL/TLS Certificates expire every 1-2 years to enforce key updates

### (v) Access Control & Role based Policies

② → Limits access to private keys based on user roles & permissions

③ → Ensures only authorized personnel or systems can access or use the keys.