Understand SSL - TLS

SSL / TLS - Secure Socket Layer / Transport Layer Security.

Cryptographic protocols designed to provide secure communication over a computer network.

**

TLS is the successor to SSL

→ SSL is deprecated ; TLS is the modern, secure version.

→ Ensure secure communication over an insecure network.

→ Provide encryption, authentication and data integrity.

→ Encrypt data and ensure its
→ integrity
→ confidentiality and
→ authenticity

between a client and server.

Methods use by TSL/SSL to achieve these principles

Principles	Methods to Achieve
Confidentiality → Data is only accessed by client / server	Encryption
Integrity → Data is not modified in between	Hashing
Authentication → Verify the identity of the parties who they are supposed to be.	Certificates

Encryption: Converting a plaintext information into a coded form (cipher text).

Eg Encrypt DEMO → GHPR
(ciphertext, each character shifted by 3 char).

Decrypt GHPR → DEMO
Shift each character by 3 backward.

Encryption Types

- Symmetric
- Asymmetric

Symmetric : Type of Encryption in which Encryption and decryption occur using the same key.

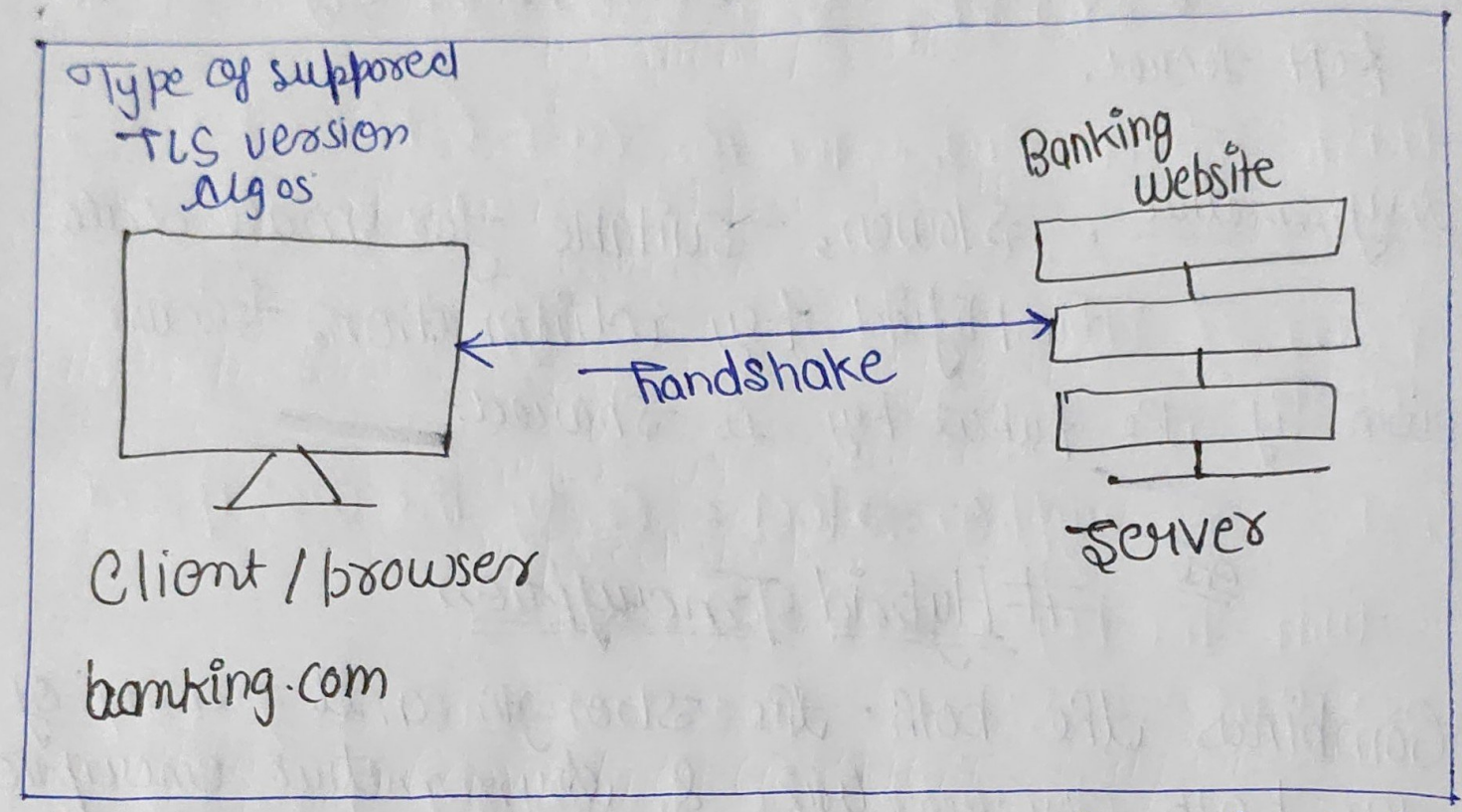
∴ Encrypt key = 3	DEMO → GHPR Shift each char by 3 forward.
∴ Decrypt key = 3	GHPR → DEMO Shift each char by 3 backward

Asymmetric : Type of Encryption in which Encryption and decryption occur using the different key

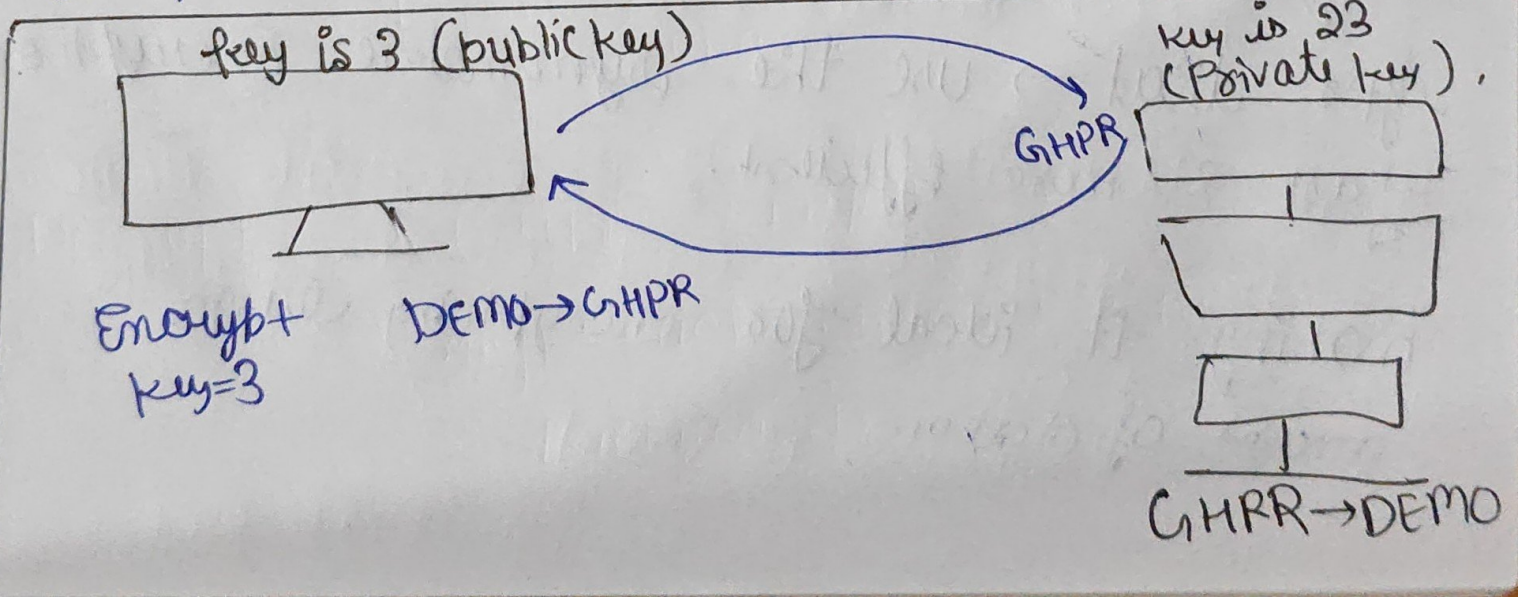
∴ Encrypt key = 3	DEMO → GHPR shift each char by 3 forward
∴ Decrypt key = 23	GHPR → DEMO Shift each char by 23 forward.

Working

Step-1 :- Initially handshanking and select Type of supported TLS version algo blw client / browser and server.



Step-2 :- Server generate two key public key & private key, public key share to client using this credential & and critical information encrypt send to server.



Symmetric Vs Asymmetric

- Symmetric : faster and more efficient, suitable for large data.
- Challenging key distribution, single key must be kept secret.

- Asymmetric : Slower, suitable for small data
  - Simplified key distribution, secure even if the public key is shared.

#Hybrid Encryption

Combines the both the strength and security of the both symmetric & asymmetric encryption to achieve efficient and secure communication.

- Asymmetric used to shared the exchange of a symmetric key.

After that → use the symmetric encryption fast & more efficient.

making it ideal for encrypting large amount of data.

Some Algo Example:-

Asymmetric	Symmetric
• DSA	• AES
• RSA	• 3DES
• ECC	• RC4
• ECDH	

#Hashing

Hashing is the process of converting data into a fixed-size string of character, as a sequence of numbers & letters.

Eg DEMO → 37 (4+5+13+15) = 37

#MAC (message Auto Code)

Combine message + secret key

Message Demo . Secret key = 123

Demokey → Server check Encryption to decryption then hashing check using the secret key.

Most Common Hashing Algo

- MD5 (Message digest Algorithm 5) (128 bits)
- SHA (Secure Hash Algorithm)
  - Sha-1
  - Sha-2/3 224 256 384 512

Hash-based Authentication code (Sha256 h mac).

how it works both Encryption & Hashing work

First: Encryption → lock = Only the recipient with the key can open it

Decryption: Server uses session key to decrypt the incomming message into plaintext first of all.

- Second: Hashing → Seal = If the message broken, you know something wrong.

HMAC Verification: Server calculates HMAC on the plaintext & compares it with the received HMAC.

→ if match = Data is valid
→ if not = Data is tampered → Reject.

#Authentication

Verify the identity of the parties who they are supposed to be. Using the Certificate Authority.

Certificate Authority :- CA is a trusted Organization that issue digital certificates to the verify the identity of websites & enable secure, encrypted communication over the internet.

CAs ensure the authenticity and integrity of the SSL certificates they provide.