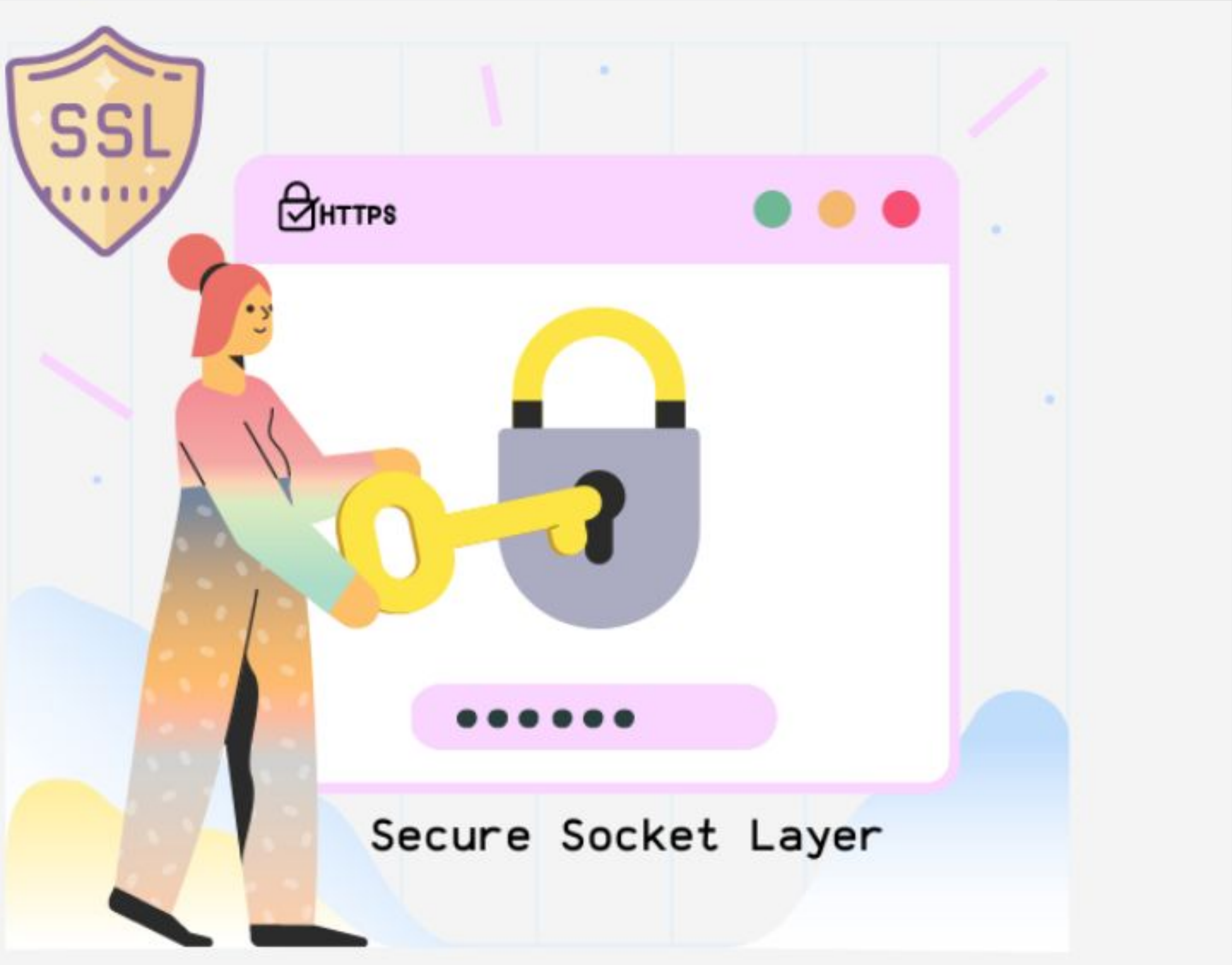
PULCHOWK ENGINEERING CAMPUS

Network security protocols : SSL/TLS



PRESENTED BY :
ALOK KARN (MSICE002)
SIDDHARTH SHARMA(MSICE017)

PRESENTED TO :
Asst. Prof. ANKU JAISWAL
NETWORK SECURITY AND ANALYSIS

Secure Socket Layer (SSL)

- Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server.

- encrypts the link between a web server and a browser which ensures that all data passed between them remain private and free from attack

- It was created by Netscape in 1995 to ensure privacy, authentication, and data integrity in online communications.

- Websites using SSL/TLS have “HTTPS” in their URL instead of “HTTP.”

WORKING OF SSL :

- **Encryption:** SSL encrypts data transmitted over the web, ensuring privacy. If someone intercepts the data, they will see only a jumble of characters that is nearly impossible to decode.

- **Authentication:** SSL starts an authentication process called a handshake between two devices to confirm their identities, making sure both parties are who they claim to be.

- **Data Integrity:** SSL digitally signs data to ensure it hasn't been tampered with, verifying that the data

How does It Works?

To start a connection, the client and server must first agree on the protocol version and cipher suite they will use.

An example of a version 1.2 cipher suite naming is TLS_DHE_RSA_AES256_SHA256.

The first portion, TLS, specifies what the cipher suite is used for. TLS is the most common reason used for cipher suites.

The second algorithm name, DHE, is the key exchange algorithm used.

RSA is the authentication algorithm.

AES256 is the bulk data encryption algorithm, and SHA256 is the MAC algorithm.

How does It Works?

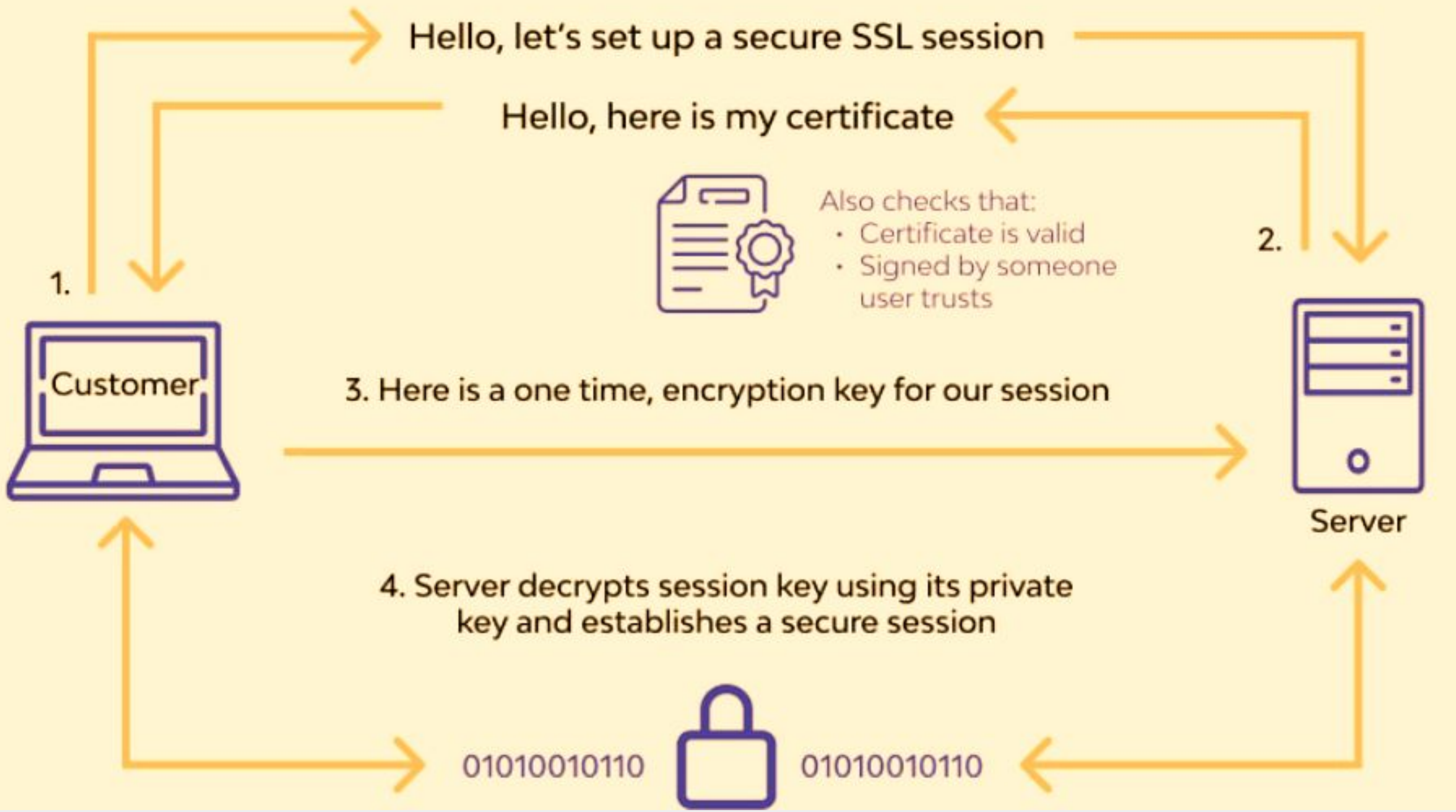
The client then sends a “Client Hello” packet which contains its supported protocol versions, cipher suites, and compression methods.

The server then sends a “Server Hello” packet with the chosen protocol version, cipher suite, and compression method.

The server will then send its SSL certificate, which contains its public key. The client generates a symmetric key using the server‘s public key to encrypt the data that is sent.

The server sends back an acknowledgement of the encryption and the client sends the data encrypted with the symmetric key.

The server receives the data, decrypts it using its private key, and sends the



Hello, let's set up a secure SSL session

Hello, here is my certificate

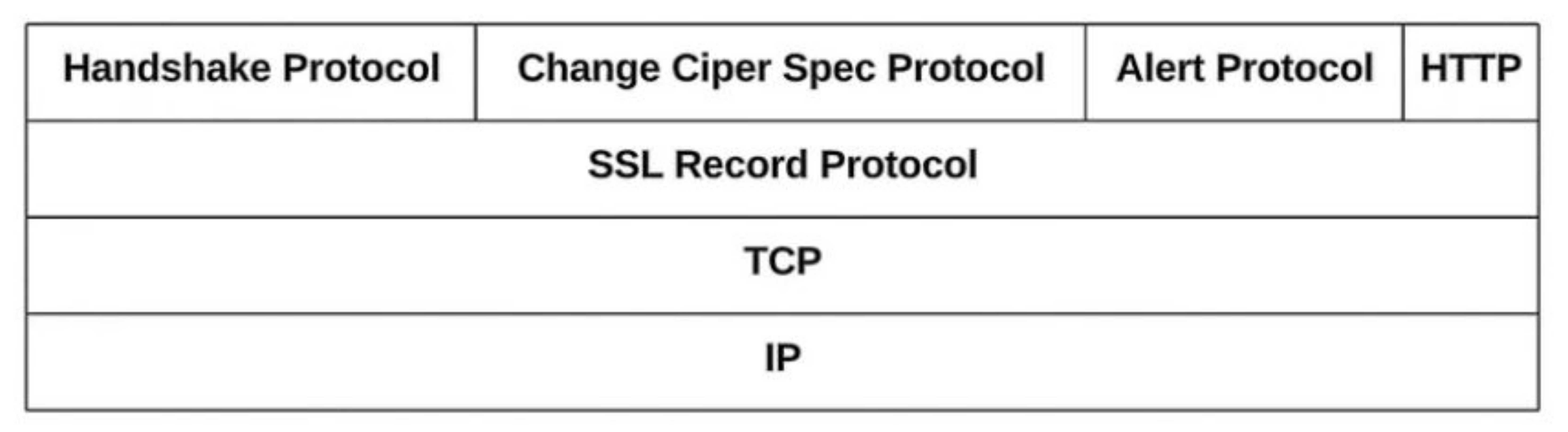
Also checks that:

- Certificate is valid
- Signed by someone user trusts

3. Here is a one time, encryption key for our session

4. Server decrypts session key using its private key and establishes a secure session

Protocols in SSL



Handshake Protocol	Change Ciper Spec Protocol	Alert Protocol	HTTP
SSL Record Protocol			
TCP			
IP			

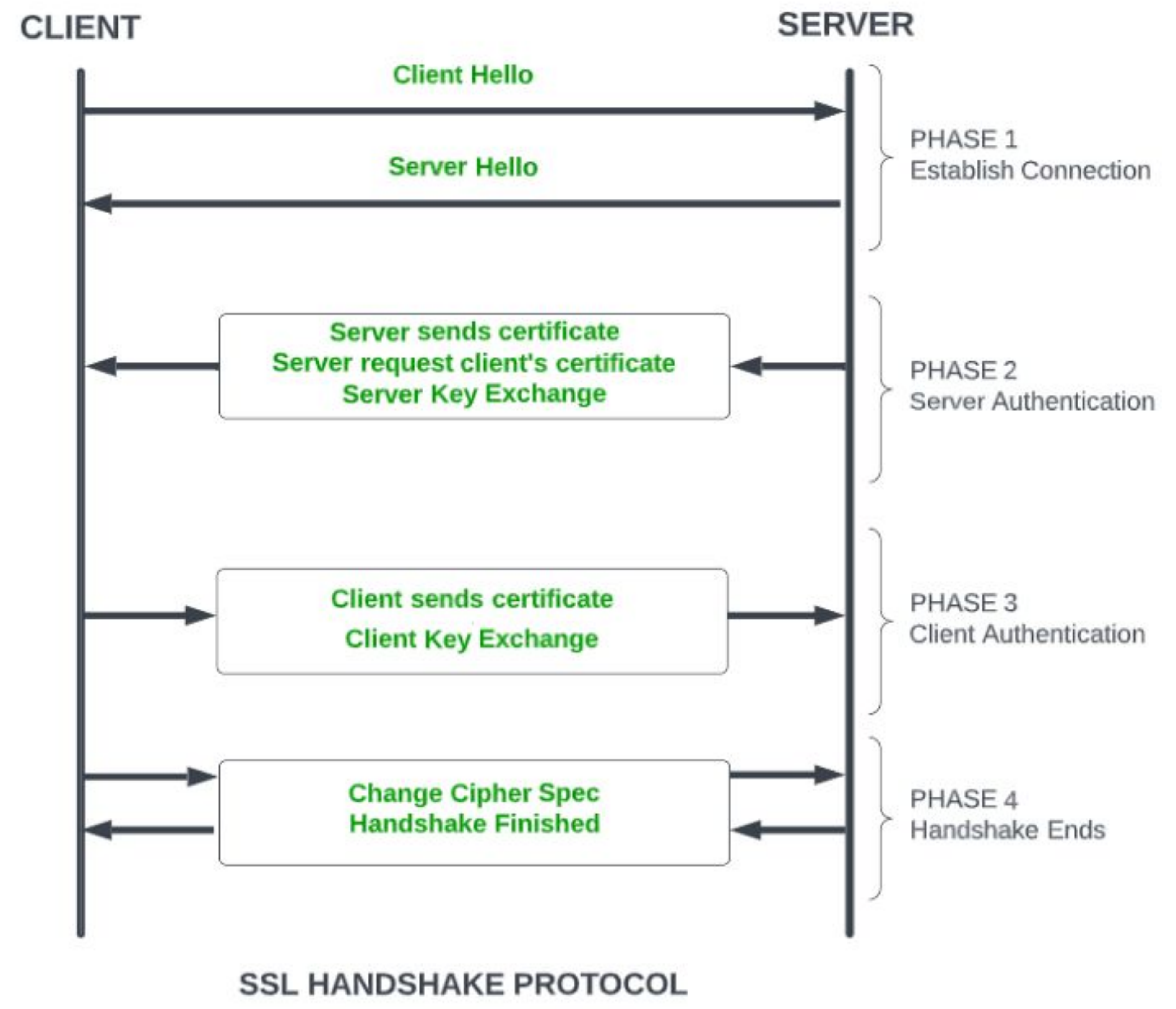
Handshake Protocol

Handshake Protocol is used to establish sessions. This protocol allows the client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

Phase-1: In Phase-1 both Client and Server send hello-pack to each other. In this IP session, cipher suite and protocol version are exchanged for security purposes.

Phase-2: Server sends his certificate and Server-key-exchange. The server end phase-2 by sending the Server-hello-end packet.

Phase-3: In this phase, Client replies to the server by sending his certificate and Client-exchange-key.



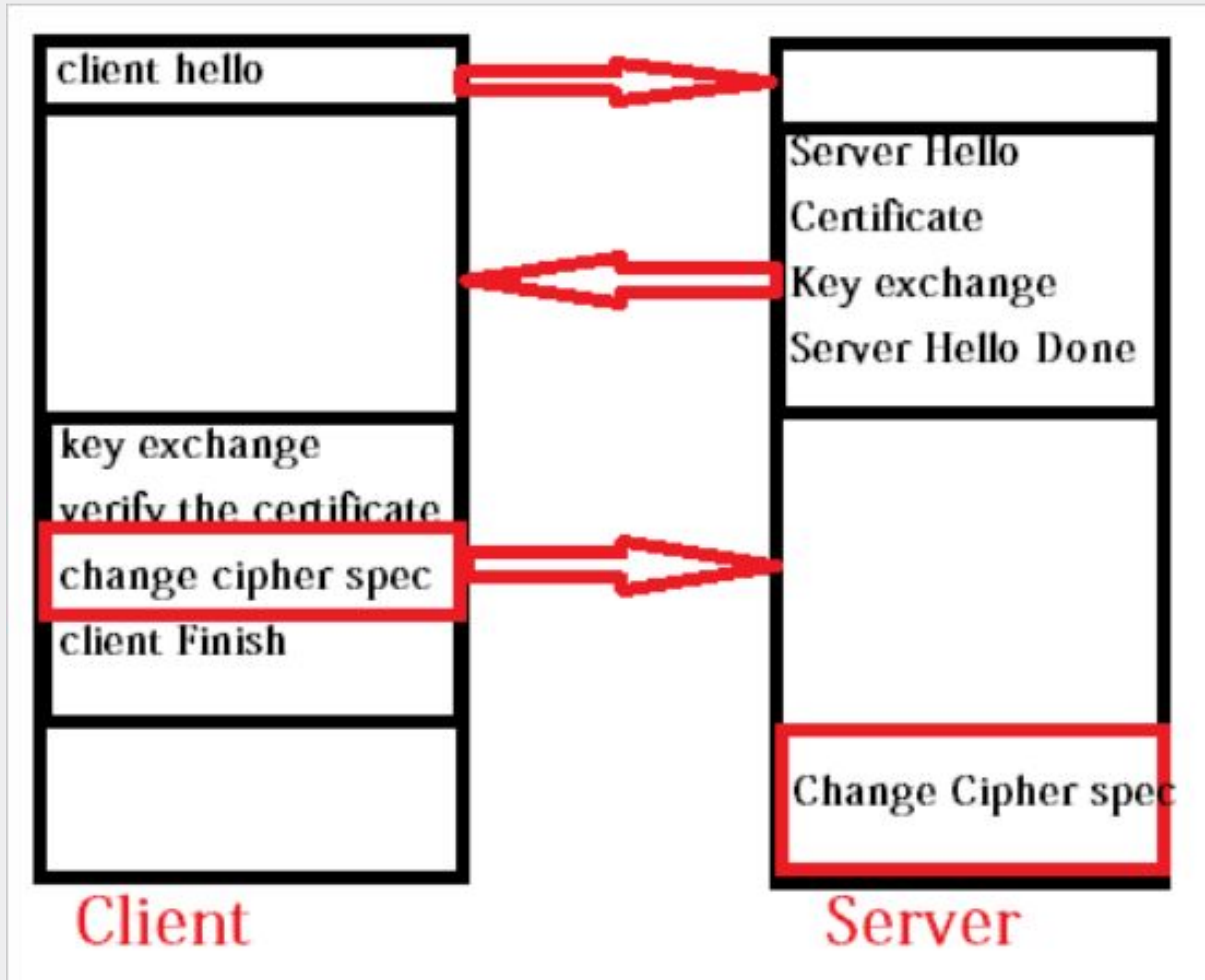
SSL Handshake Protocol Phases diagrammatic representation

Change-cipher Protocol :

Operating in conjunction with the SSL record protocol, this protocol ensures that until the Handshake Protocol is fully executed, the SSL record output remains in a pending state.

Upon completion of the Handshake Protocol, the pending state is transitioned into the current state.

The Change-cipher protocol comprises a single message with a length of 1 byte, having only one possible value. Its primary function is to facilitate the transfer of the pending state to the current state.



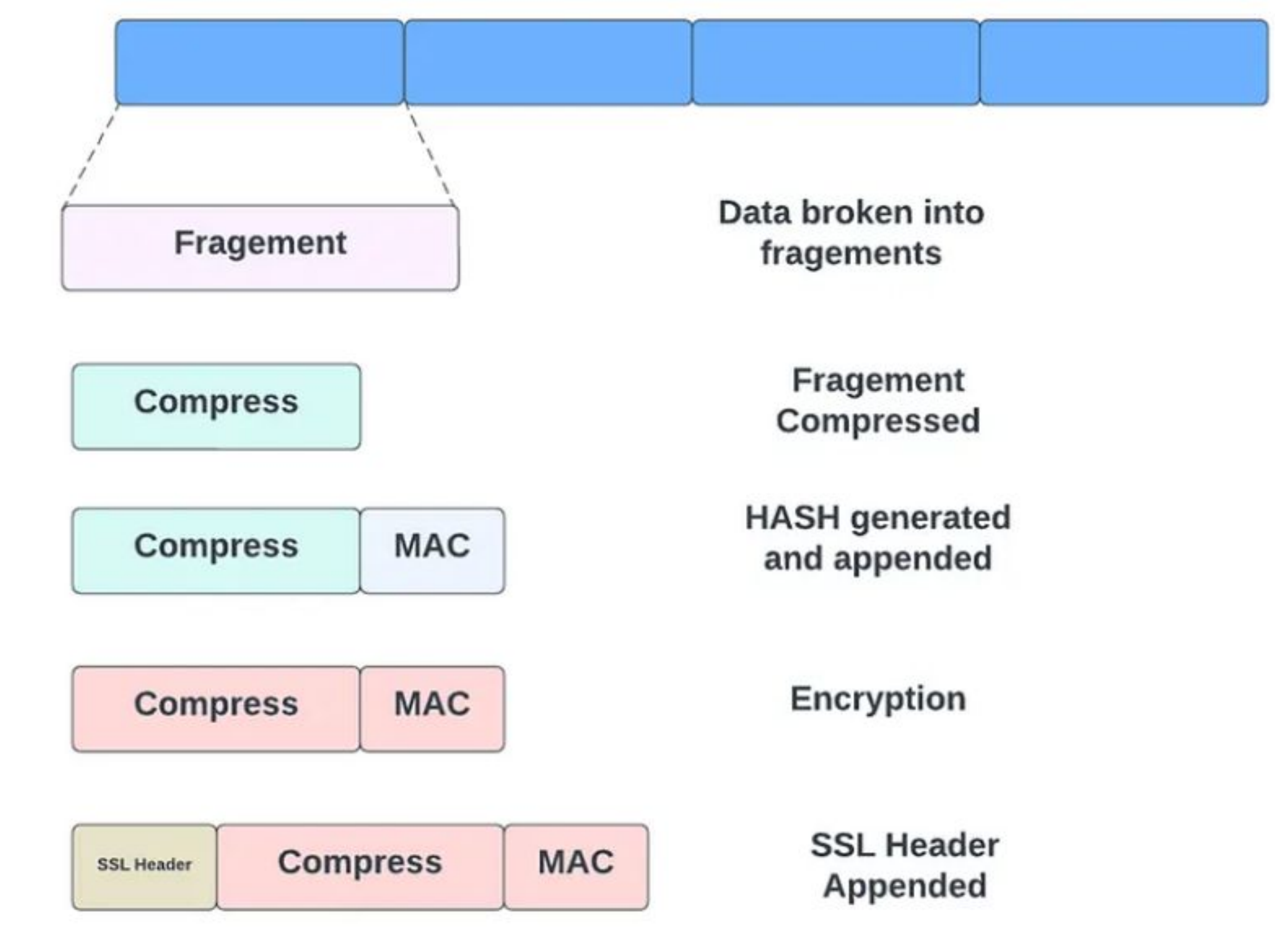
SSL Record Protocol

The SSL Record Protocol offers two crucial services to SSL connections:

- Confidentiality
- Message Integrity

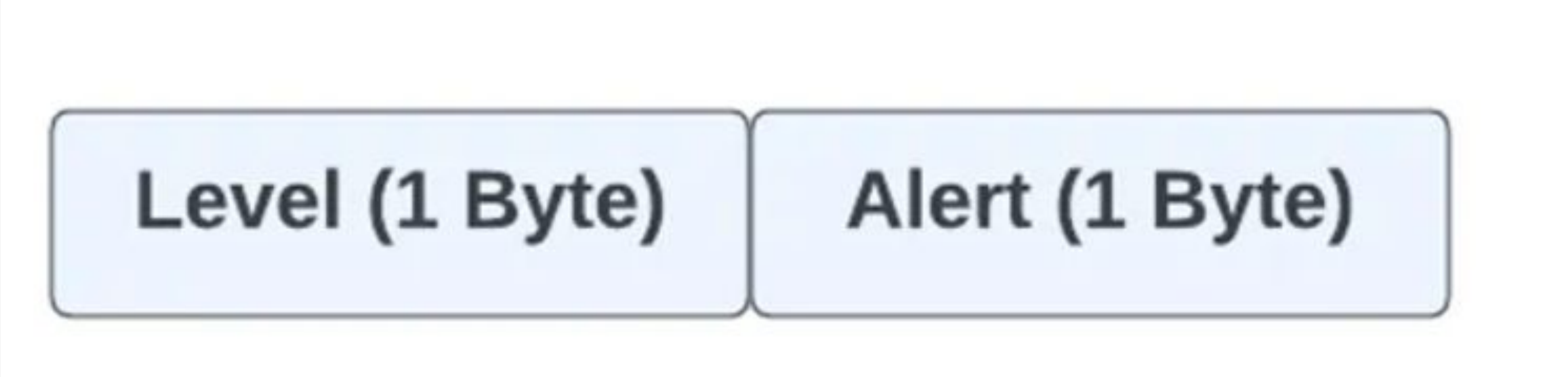
Within the SSL Record Protocol, application data undergoes fragmentation.

These fragments are compressed and then coupled with an encrypted Message Authentication Code (MAC) generated by algorithms such as SHA (Secure Hash Protocol) and MD5 (Message Digest). Following this, the data undergoes



Alert Protocol :

Designed to communicate SSL-related alerts to the peer entity, each message within this protocol consists of 2 bytes.



Level (1 Byte)	Alert (1 Byte)

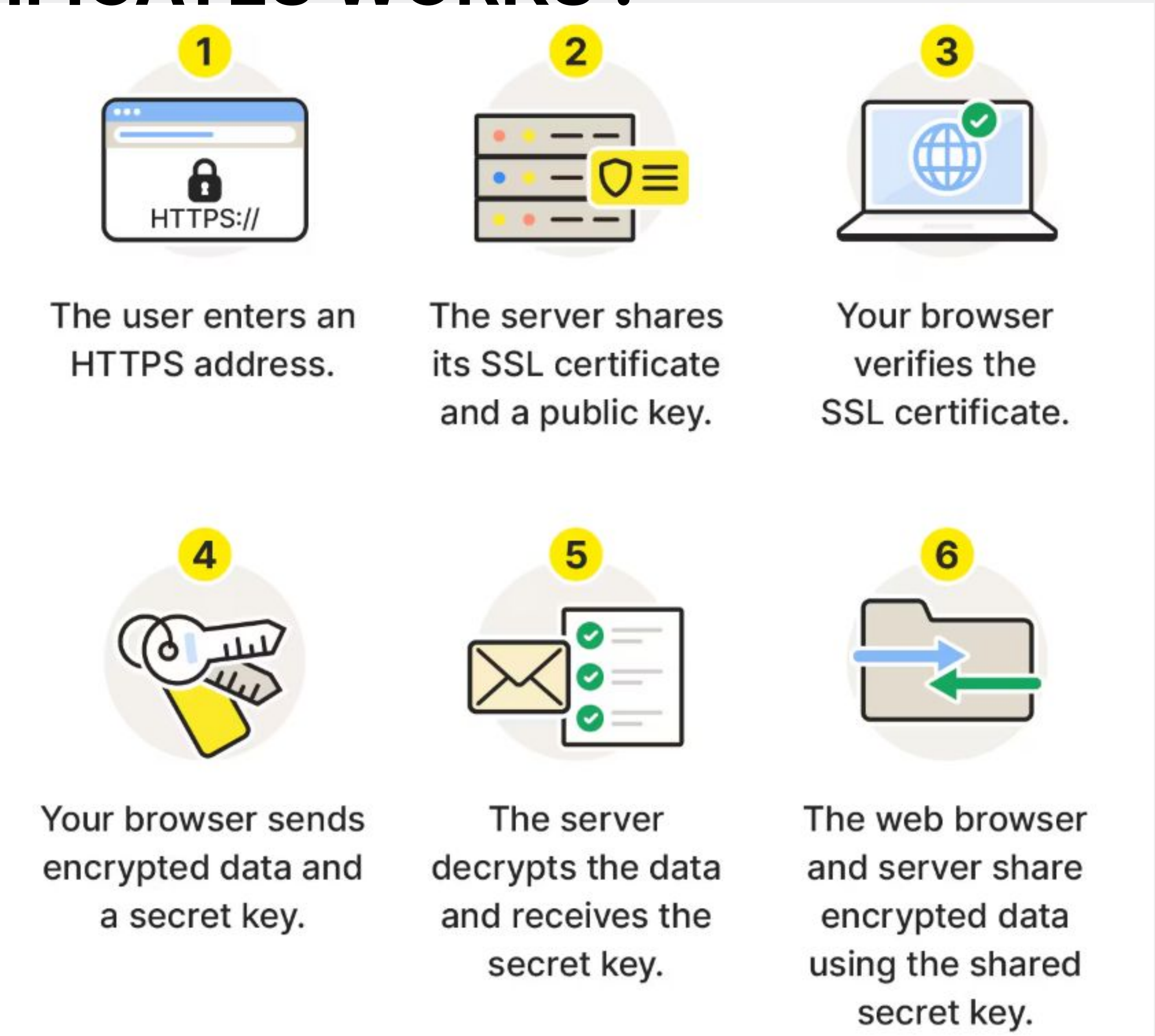
SSL CERTIFICATES :

- An SSL certificate is a digital certificate that encrypts the traffic between a user’s browser and a website’s server.

- By encrypting the data moving between a site and a user, SSLs help you browse and shop more safely online.

- SSL certificates are what enable websites to use HTTPS, which is more secure than HTTP. An SSL certificate is a data file hosted in a website's origin server

HOW SSL CERTIFICATES WORKS :



1. The user enters an HTTPS address.

2. The server shares its SSL certificate and a public key.

3. Your browser verifies the SSL certificate.

4. Your browser sends encrypted data and a secret key.

5. The server decrypts the data and receives the secret key.

6. The web browser and server share encrypted data using the shared secret key.

TYPES OF SSL CERTIFICATES:

There are three main types of SSLs:

- Extended Validation,
- Organization Validation,
- Domain Validation.

The main differences have to do with what information is needed to secure each type. Extended Validation certificates require the most information, while Domain Validation certificates require the least.

This generally means that the more information-heavy certificates are more trustworthy because of the depth of information required to earn one.

Each SSL certificate contains the following information:

- Domain name
- The company, person, or device that owns the certificate
- Subdomain names
- The issuing certificate authority (CA)
- The CA’s digital signature
- Issuance date
- Expiration date
- The public key (the private key is kept a secret)

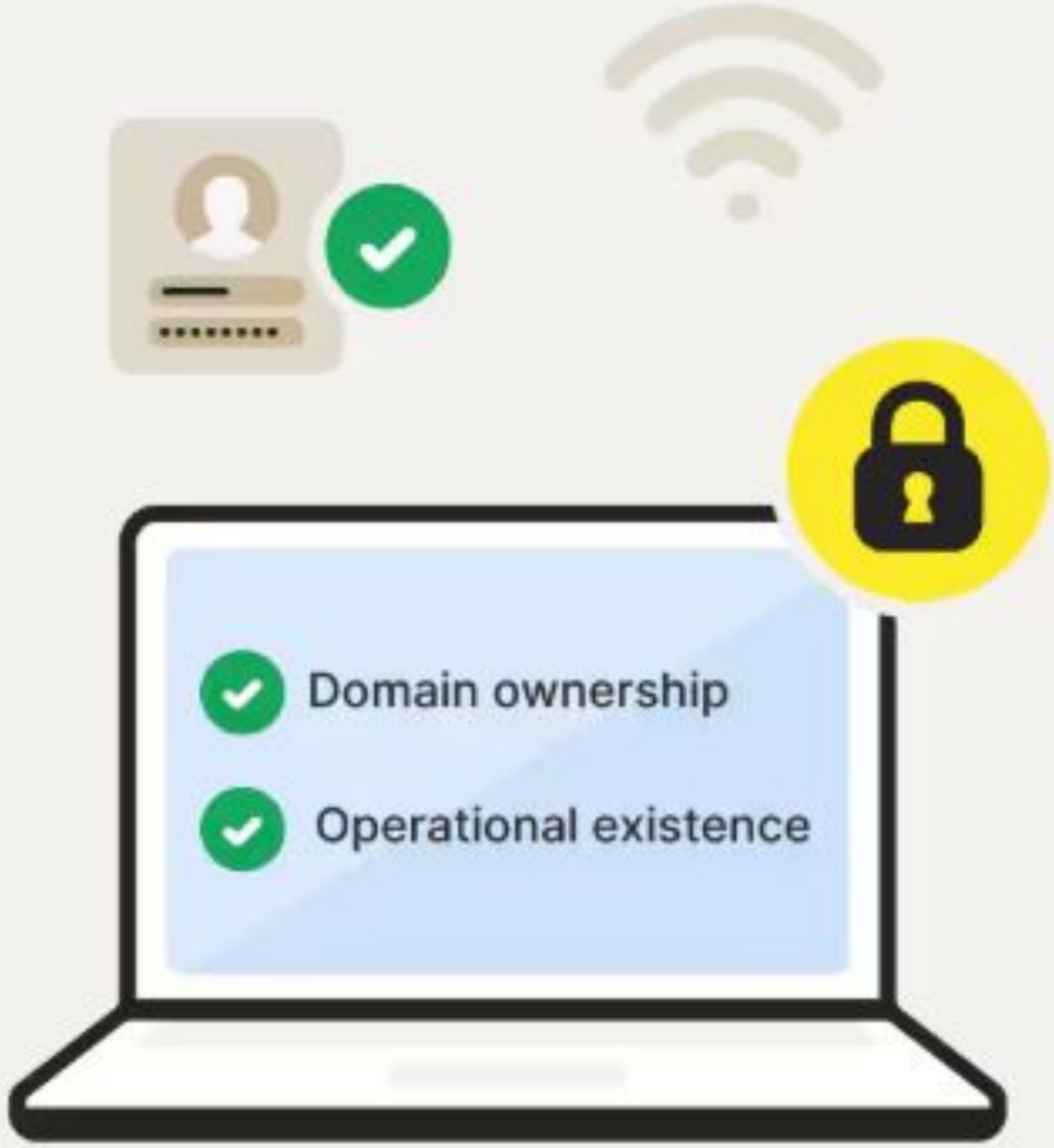
Extended Validation Certificates (EV SSL)

- Requires the most extensive vetting for certification
- The safest SSL due to the review process
- Useful for large brands, financial institutions, or other organizations handling sensitive data

- ✓ Domain ownership
- ✓ Owner information
- ✓ Physical location
- ✓ Legal status
- ✓ Operational existence

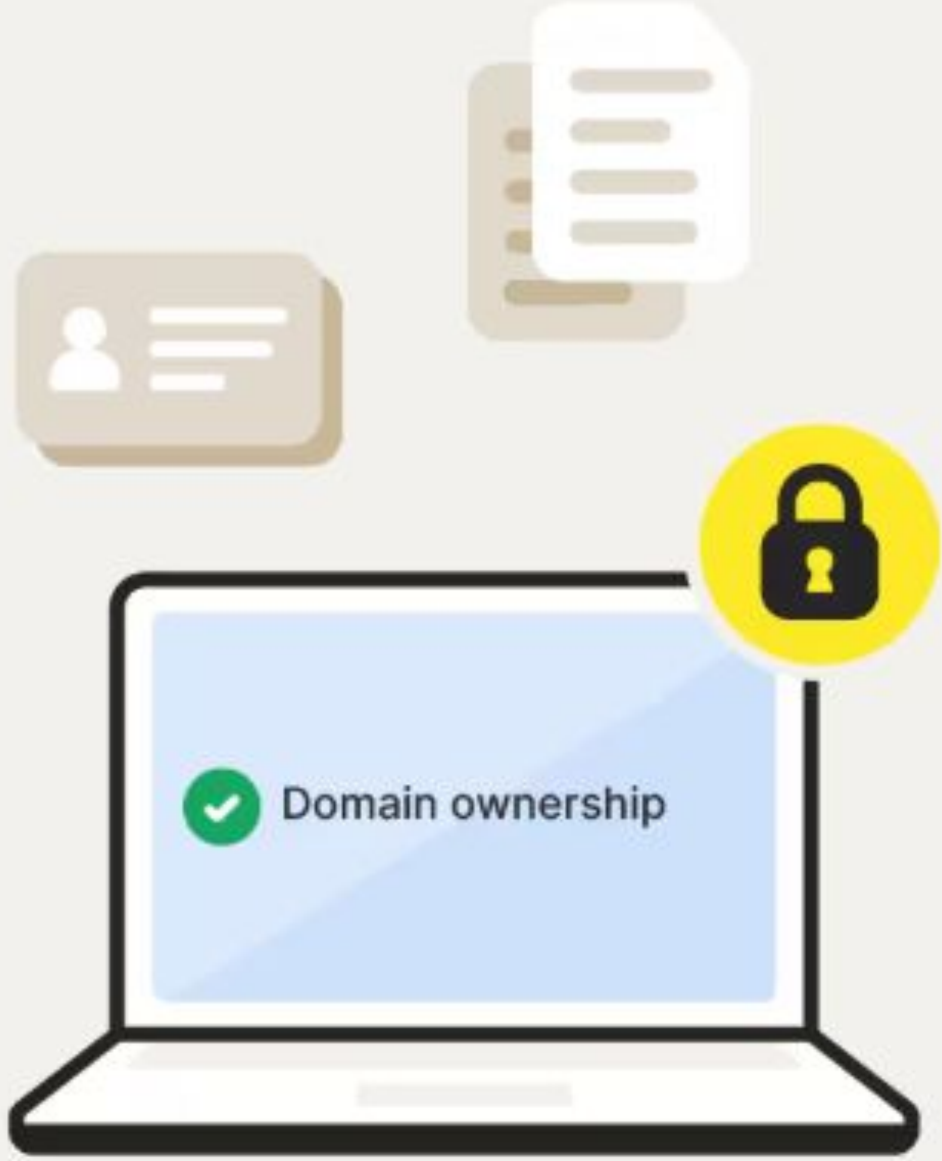
Organization Validated Certificates (OV SSL)

- Useful for sites that need security but aren’t public-facing, like intranets
- Issuing authority verifies ownership of the domain as well as the existence of an organization



Domain Validation Certificates (DV SSL)

- Easy to obtain; only checks that the domain is owned by the person requesting the certificate
- Useful for small businesses, blogs, and personal websites
- The least safe kind of SSL because they are so easy to get



Why Websites Should Have SSL Certificates

- Keep data safe
- Earn user trust
- Meet PCI DSS standards
- Prevent fake versions of a site
- Can improve search engine rankings

TLS(TRANSPORT LAYER SECURITY)

TLS :

- cryptographic protocol designed to provide secure communication over computer network.

- TLS is the successor to SSL

- Transport Layer Securities (TLS) are designed to provide security at the transport layer.

- TLS ensures that no third party may eavesdrop or tampers with any message.

how TLS secure data ?

encrypt data and ensures its

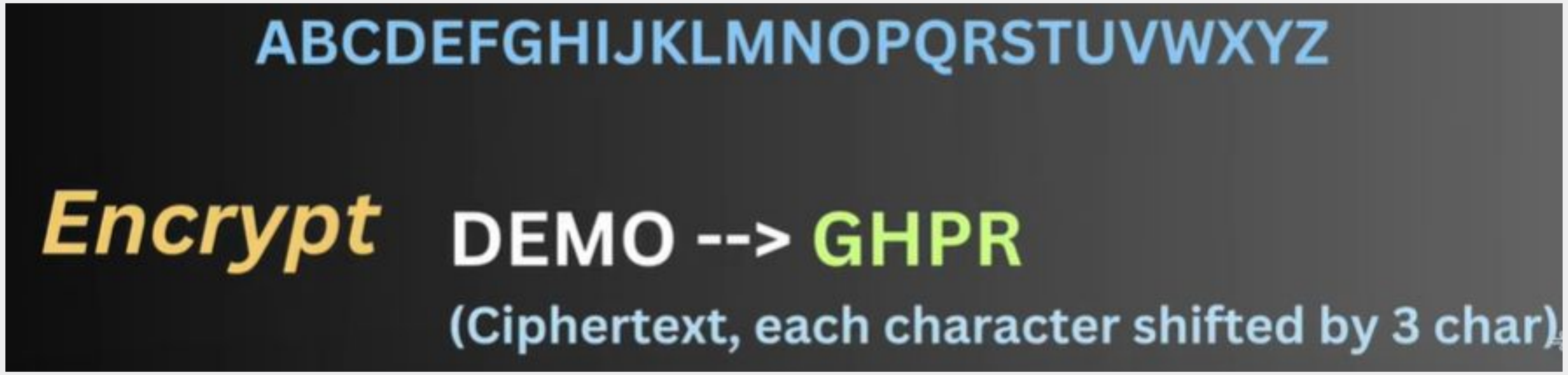
- integrity
- confidentiality
- authenticity

between server and client

CONFIDENTIALITY	DATA IS ONLY ACCESSED BY CLEINT SERVER	ENCRYPTION
INTEGRITY	DATA IS NOT MODIFIED IN BETWEEN	HASHING
AUTHENTICATION	VERIFYING THE IDENTIITIES OF THE PARTY WHO ARE THEY SUPPOSED TO BE	CERTIFICATES

ENCRYPTION

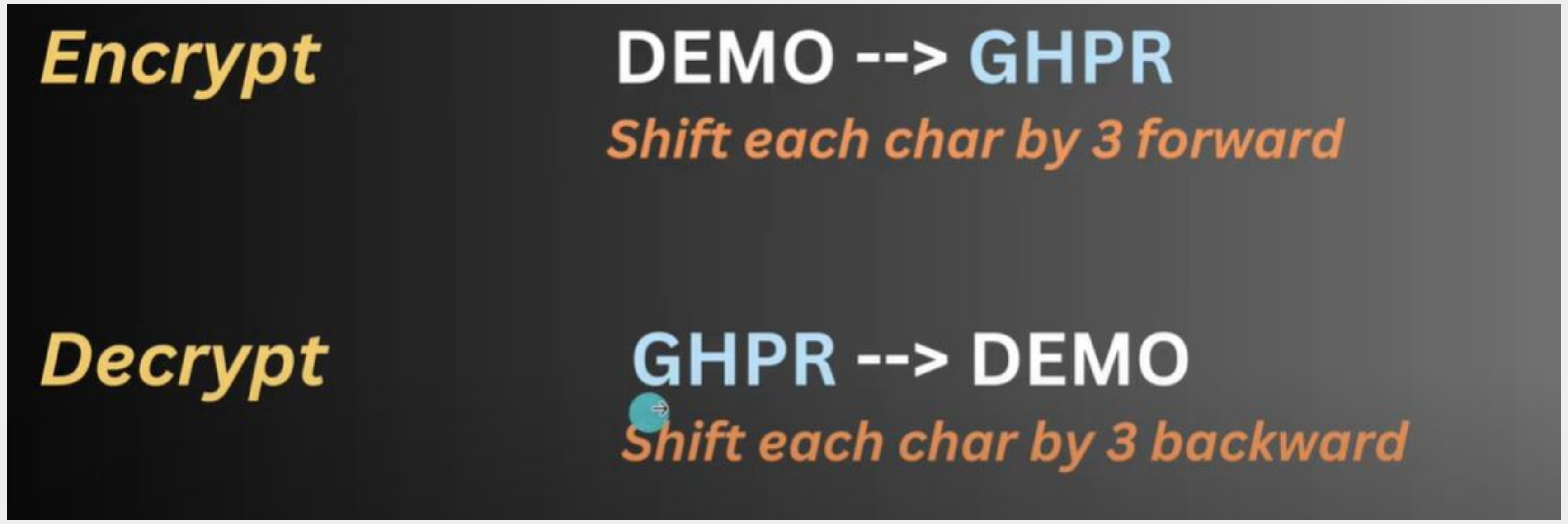
CONVERTING PLAINTEXT INFORMATION INTO CODED FORM (CIPHER)



ABCDEFGHIJKLMNOPQRSTUVWXYZ

Encrypt DEMO --> GHPR

(Ciphertext, each character shifted by 3 char)

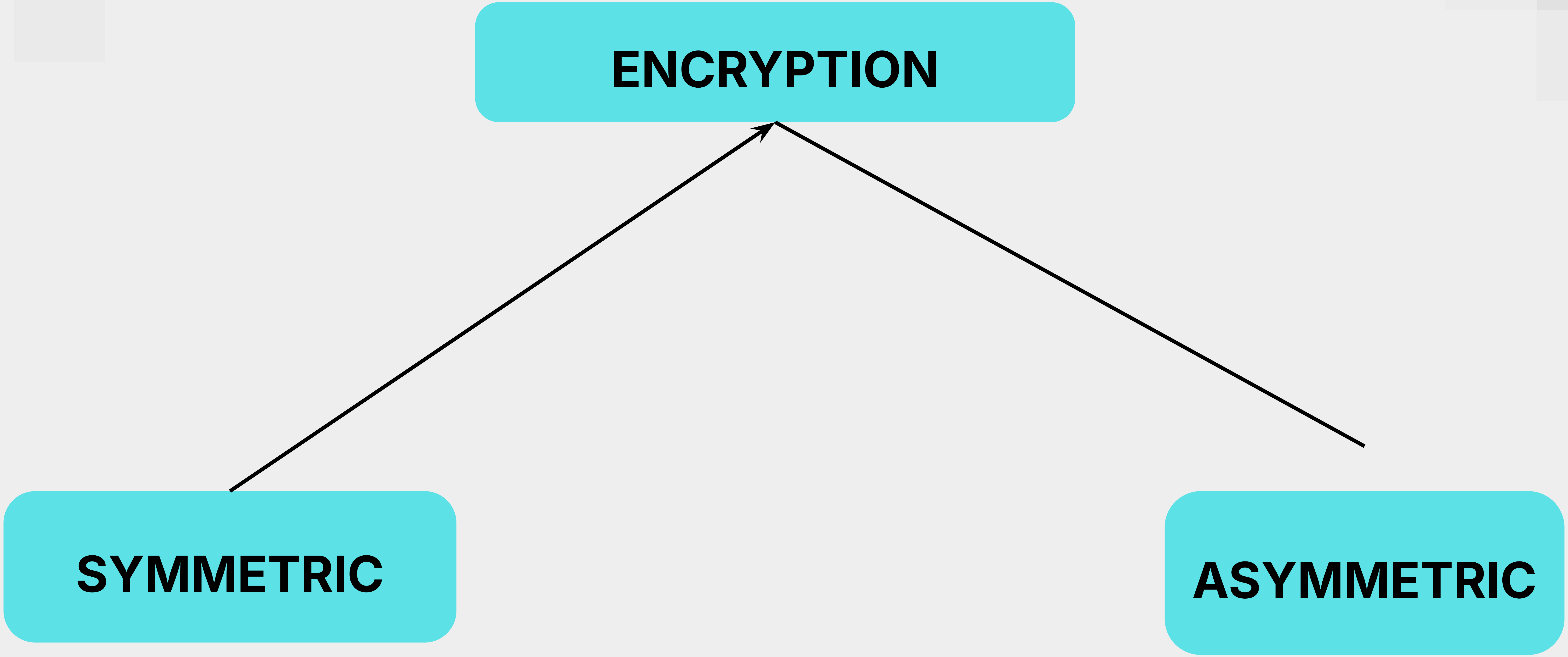


Encrypt DEMO --> GHPR

Shift each char by 3 forward

Decrypt GHPR --> DEMO

Shift each char by 3 backward

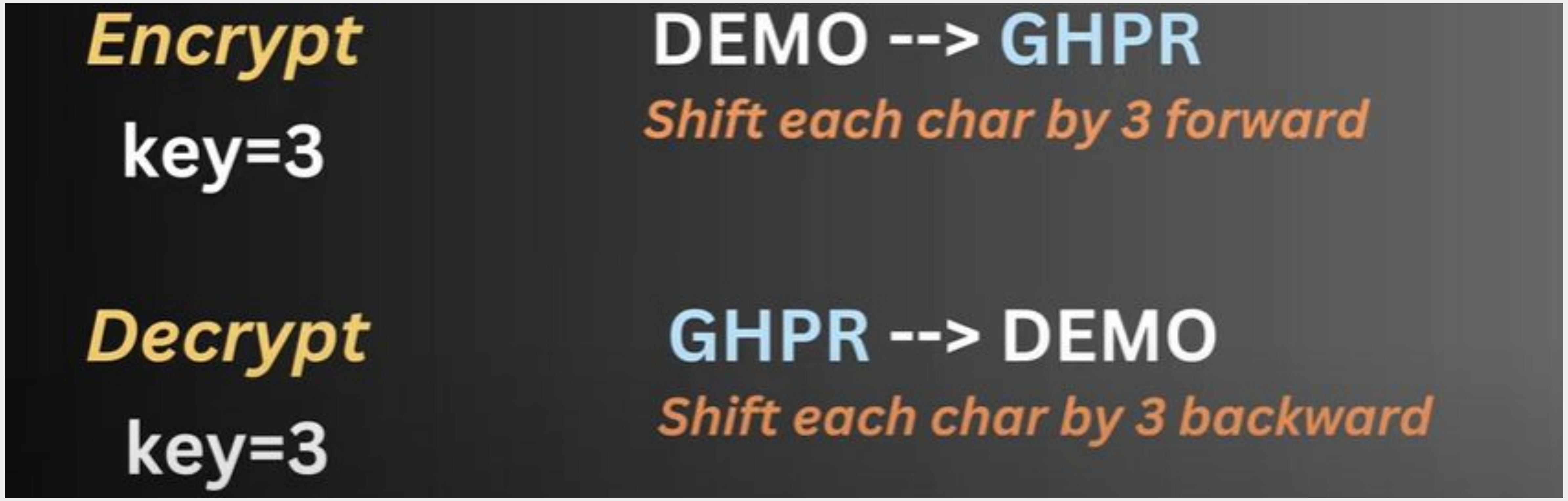


ENCRYPTION

SYMMETRIC

ASYMMETRIC

SYMMETRIC ENCRYPTION:



Encrypt

key=3

DEMO --> GHPR

Shift each char by 3 forward

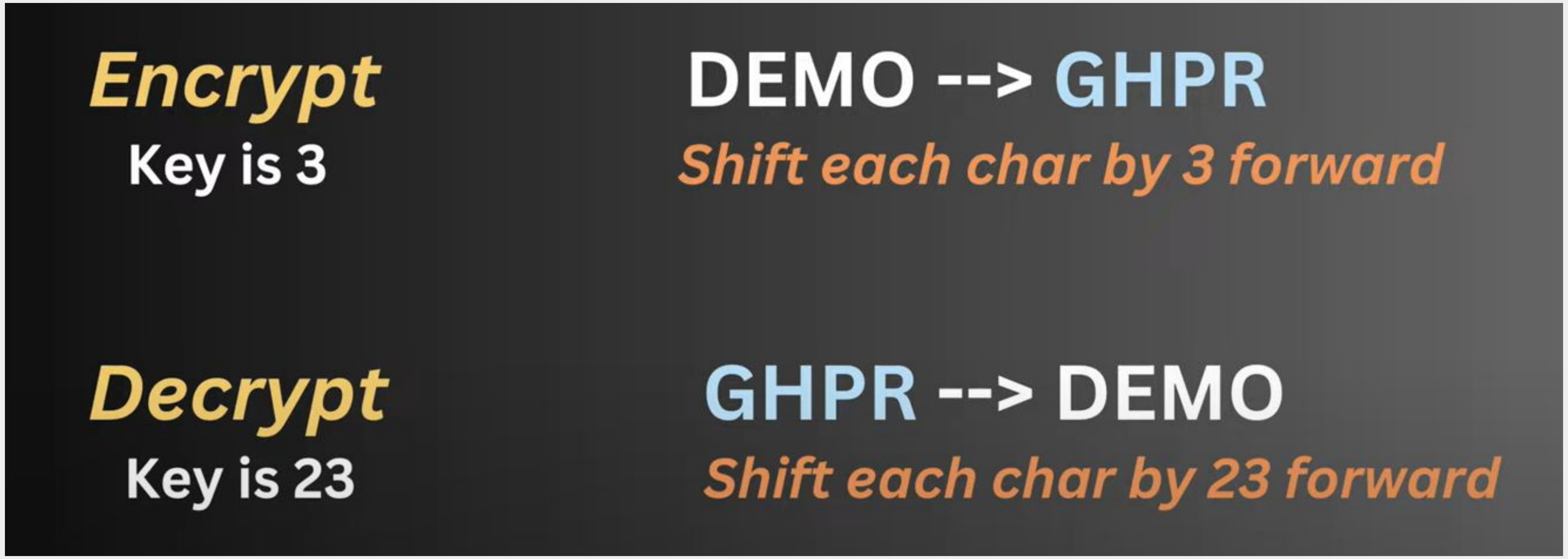
Decrypt

key=3

GHPR --> DEMO

Shift each char by 3 backward

ASYMMETRIC ENCRYPTION:

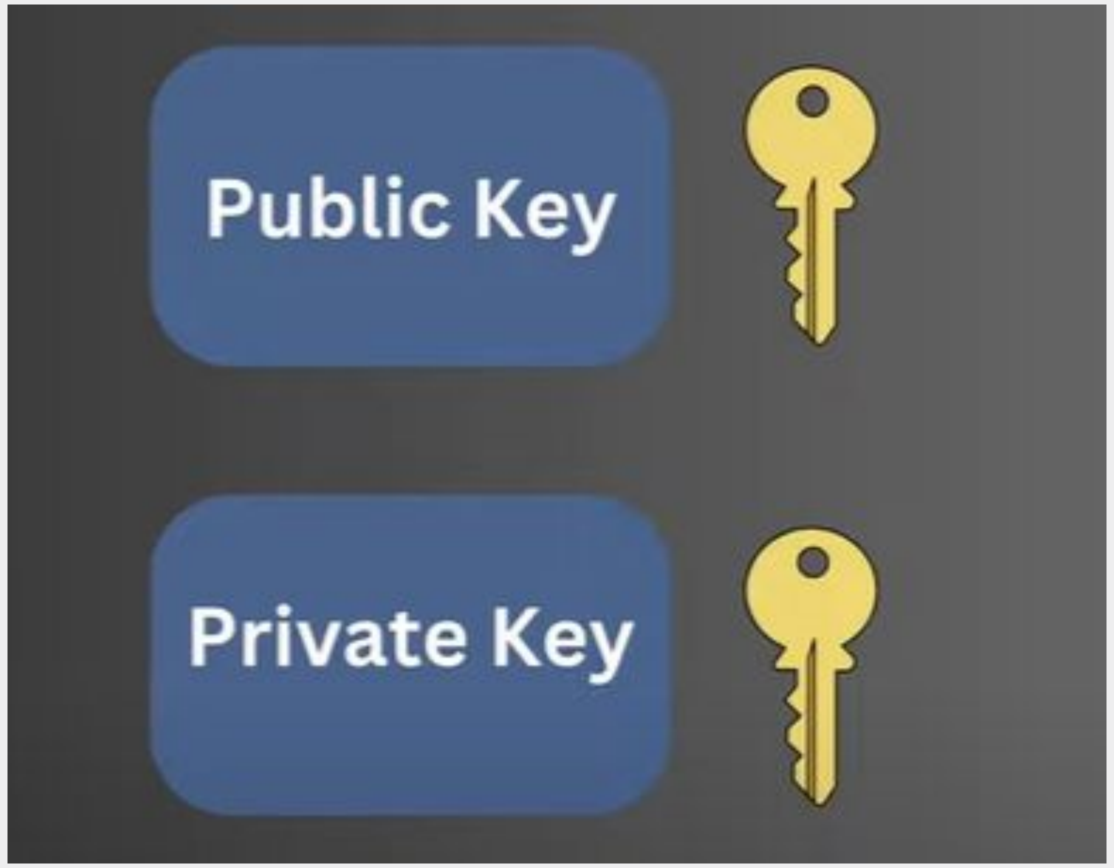


Encrypt
Key is 3

DEMO --> GHPR
Shift each char by 3 forward

Decrypt
Key is 23

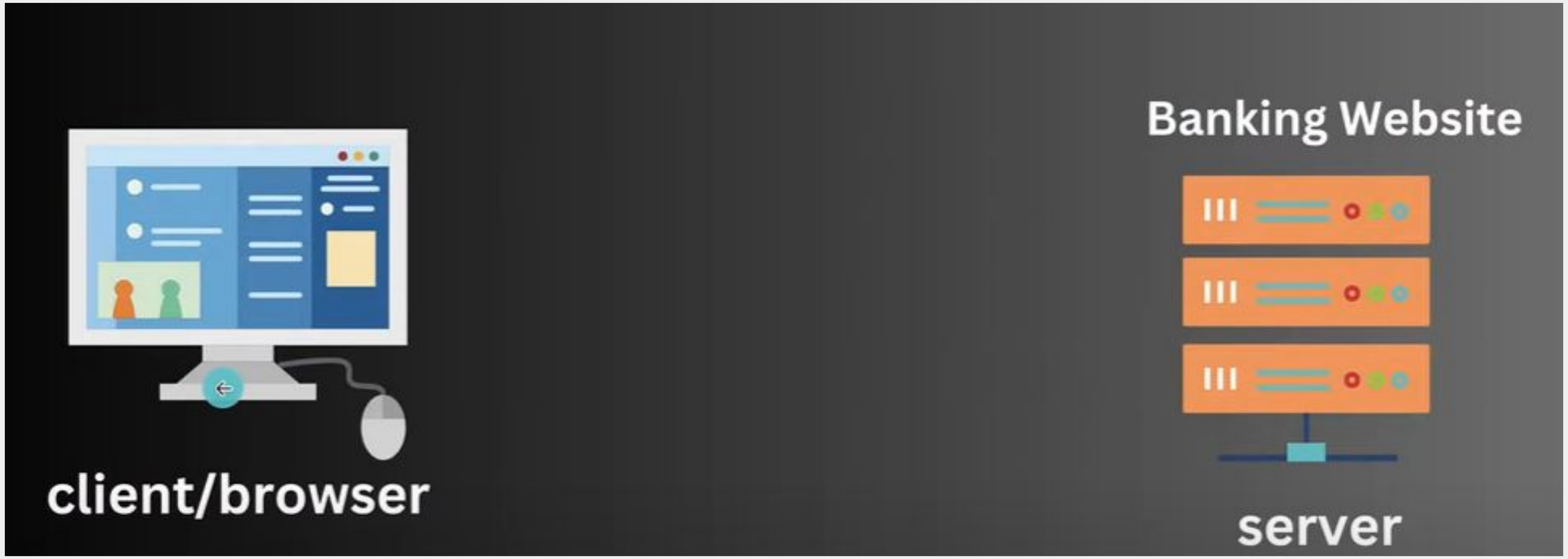
GHPR --> DEMO
Shift each char by 23 forward

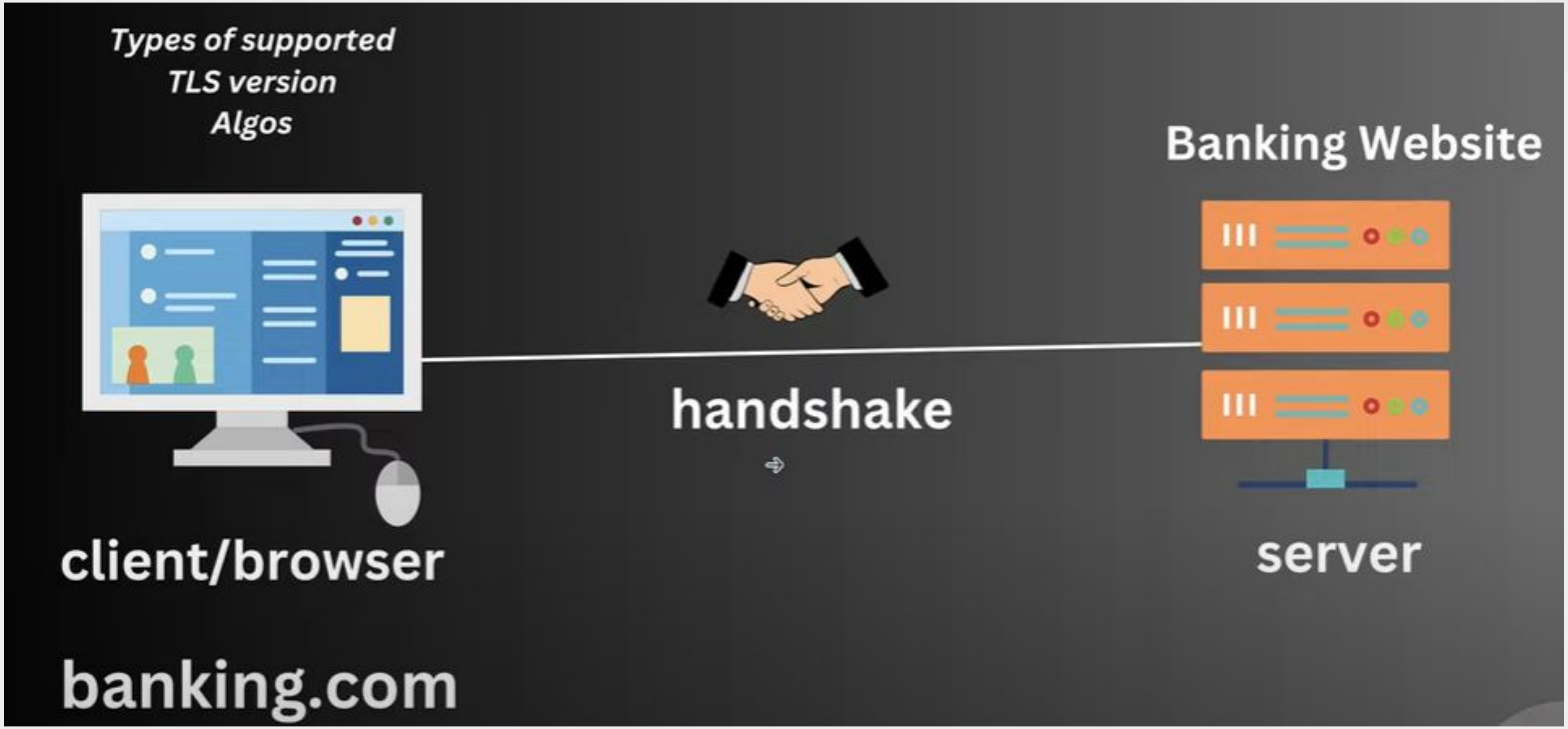


Public Key

Private Key

Now, let’s understand this with a real life flow :





Types of supported
TLS version
Algos

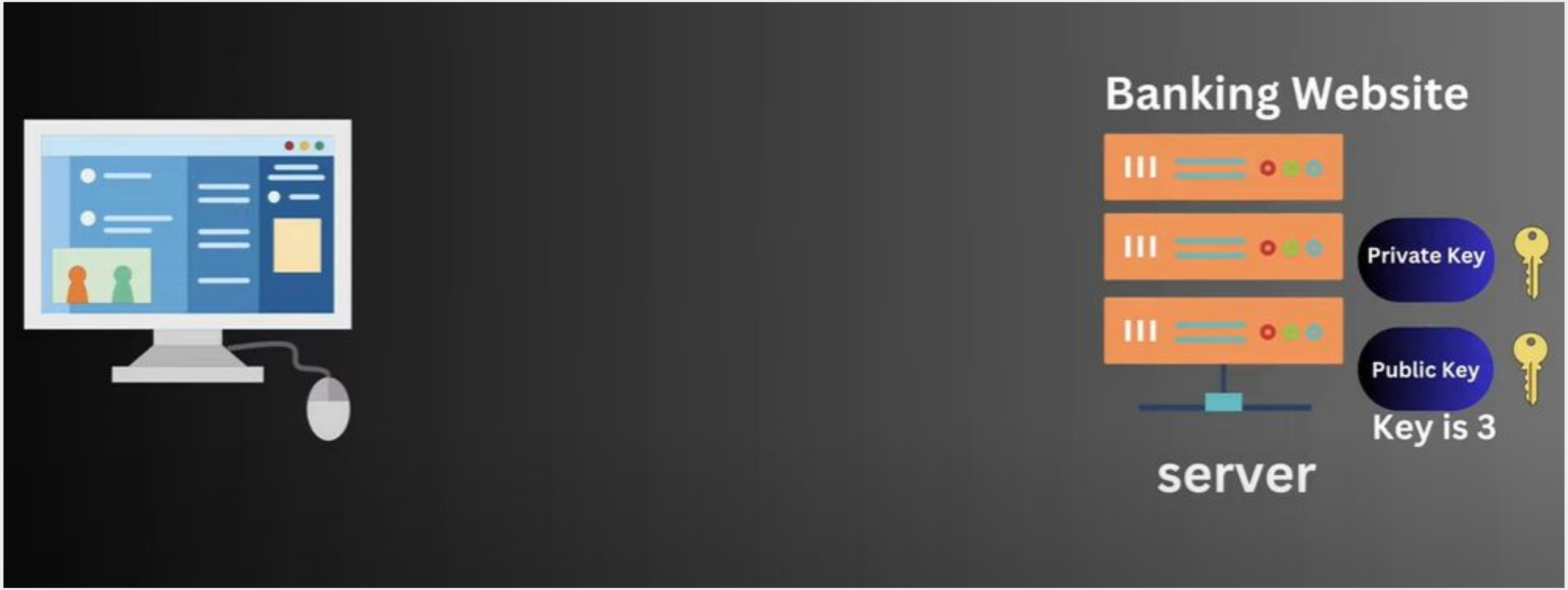
Banking Website

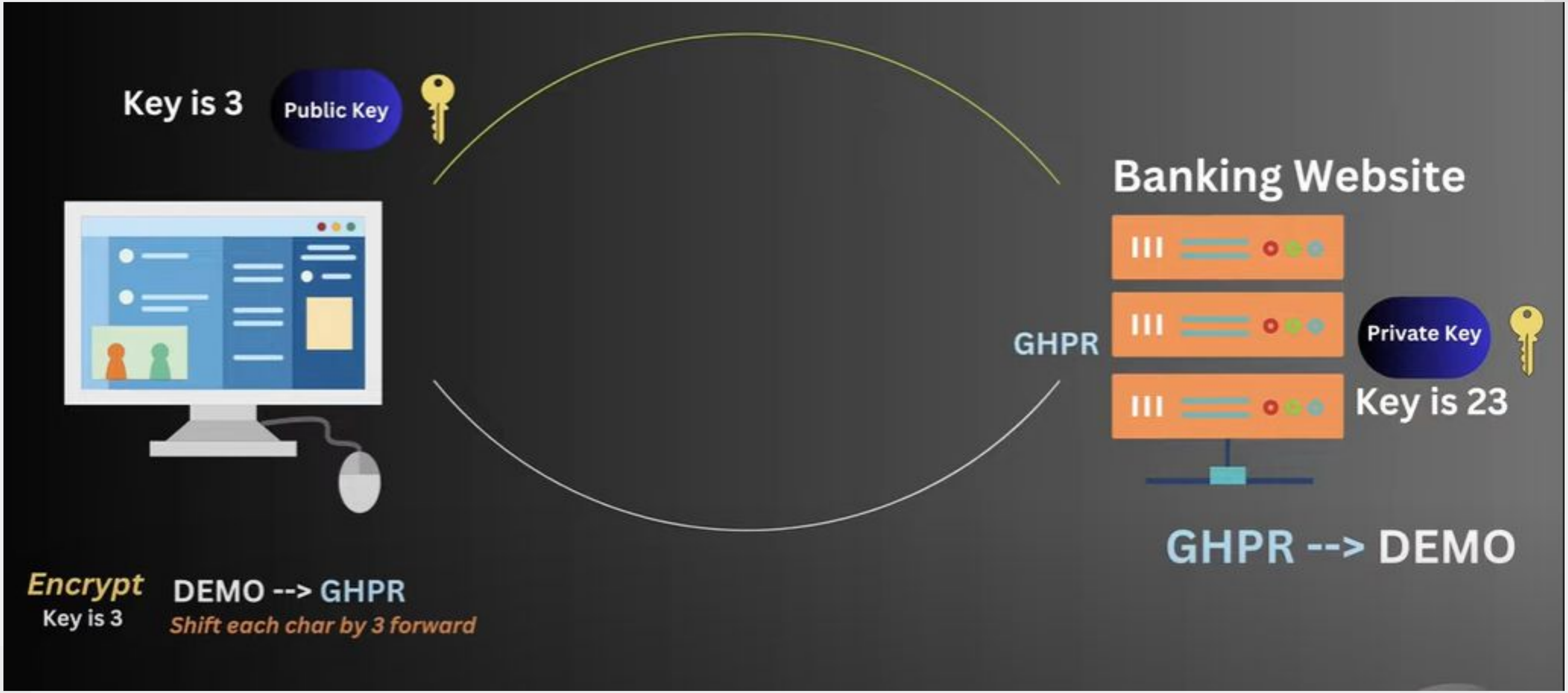
handshake

client/browser

server

banking.com


Banking Website
Private Key
Public Key
Key is 3
server



Key is 3

Public Key

Banking Website

GHPR

Private Key

Key is 23

GHPR --> DEMO

Encrypt

Key is 3

DEMO --> GHPR

Shift each char by 3 forward

Some encryption algorithm examples

SYMMETRIC

- DSA
- RSA
- ECC
- ECDH

ASYMMETRIC

- AES
- 3DES
- RC4

How real life AES encryption looks like...

Message: DEMO

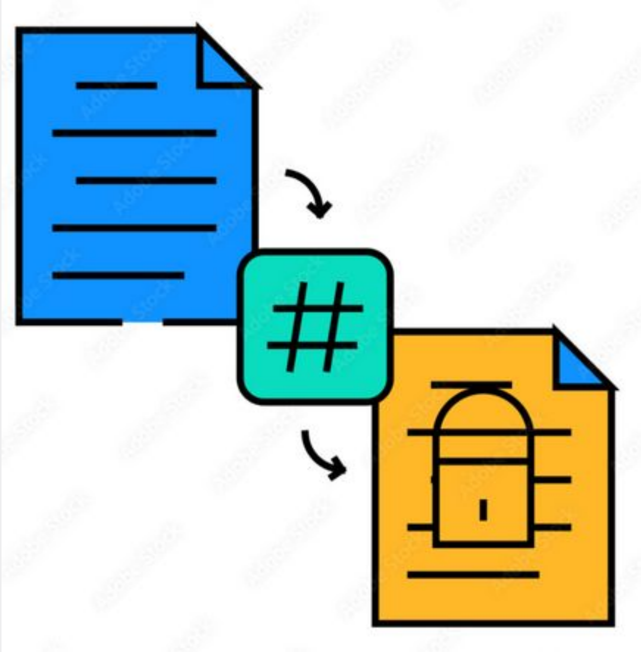
Key 256 bit HEX:
cb5a6cefcf5b7e88f9bff6f27f32d6095a86db829d8518cf8edb6af274
0ff8eb

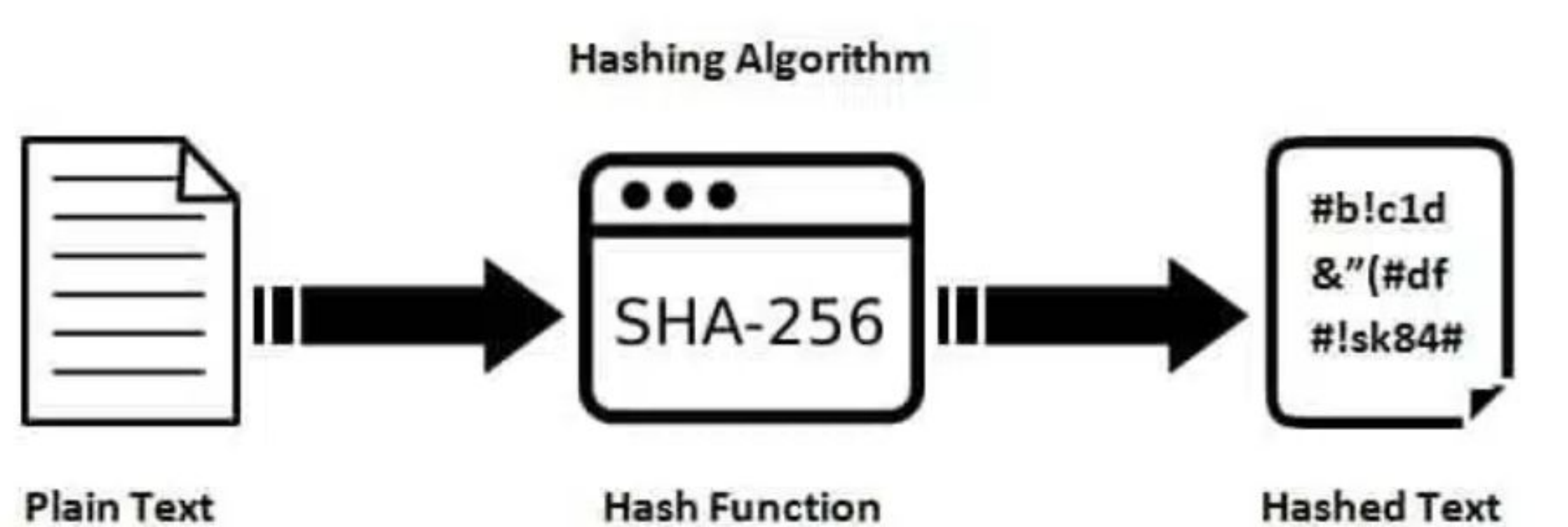
Initialiation Vector (IV) : (a8d246bb6ebae2b0e7651843b3053384

AES-256-CBC Encryption:8?Q3?B??Z)?07h??

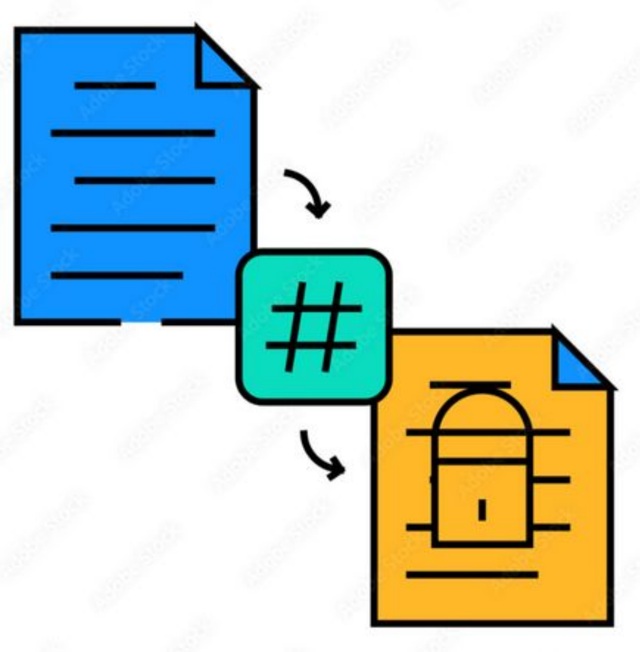
HASHING

- MAINTAINS INTEGRITY
- TO ENSURE WHETHER THE DATA IS MODIFIED OR NOT





HASHING

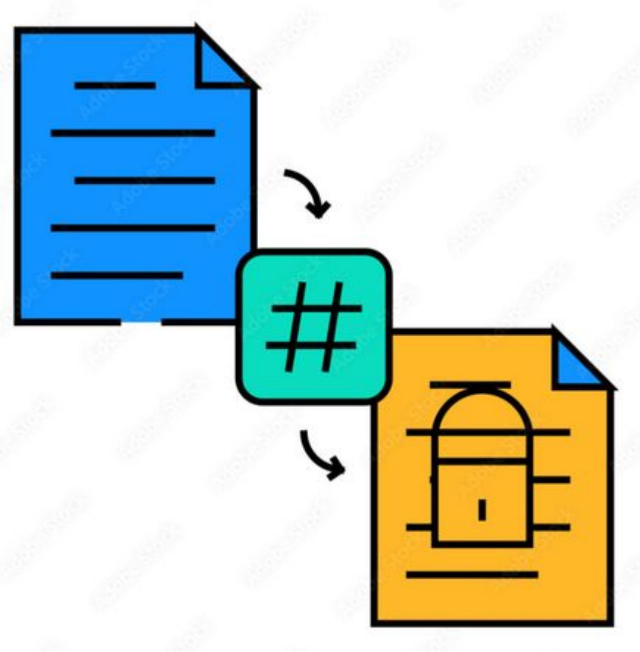


Hashing is the process of converting data into a fixed sized string of characters, as a sequene of function and characters .

Eg:

DEMO → 37 (4+5+13+15=37)

ABCDEFGHIJKLMNOPQRSTUVWY Z



MOST COMMON HASHING ALGORITHM :

- MD5(MESSAGE DIGEST ALGORITHM 5)

- SHA(SECURE HASHING ALGORITHM)

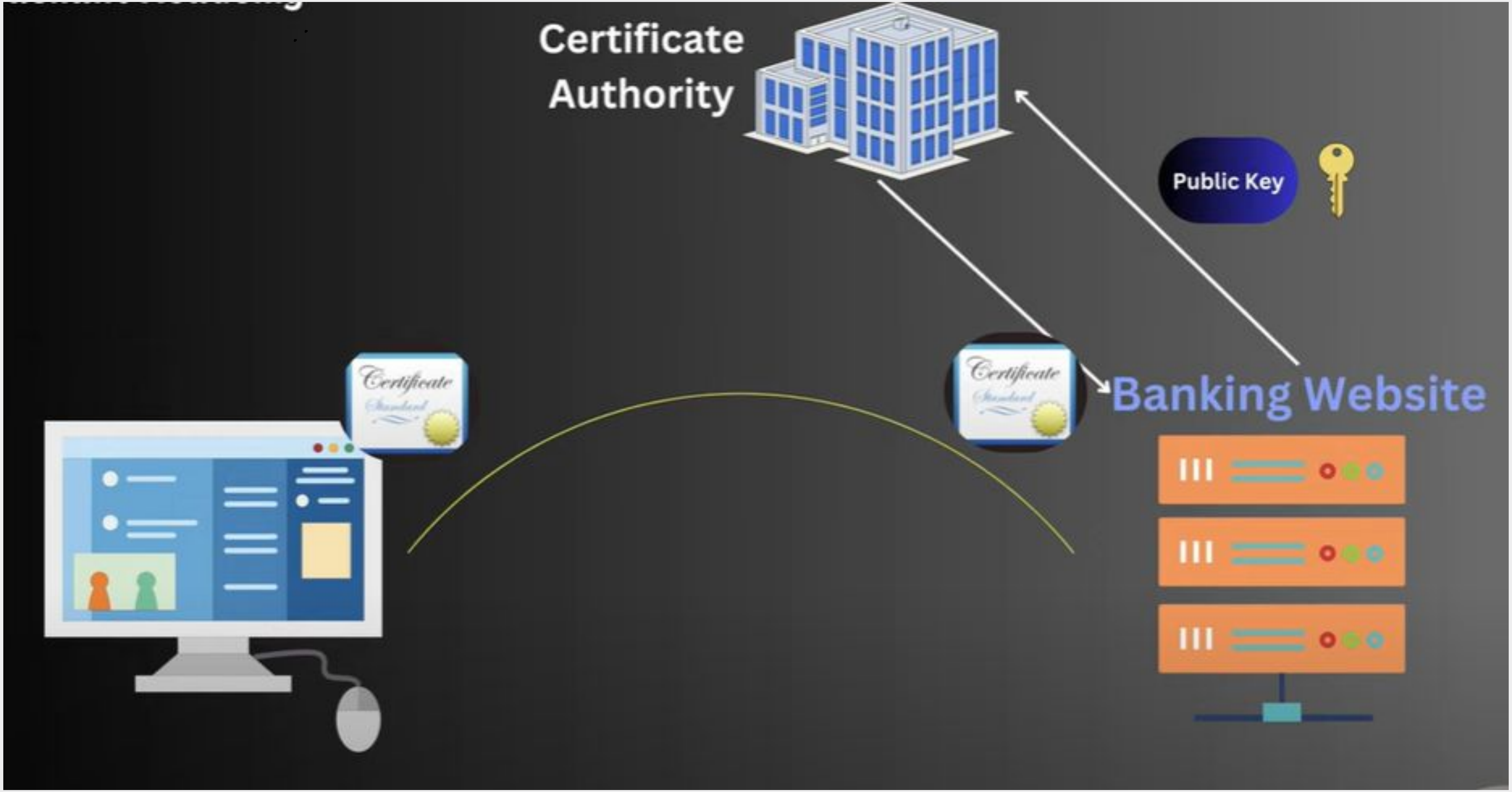
- SHA-1
- SHA-2/3 224 256 384 512

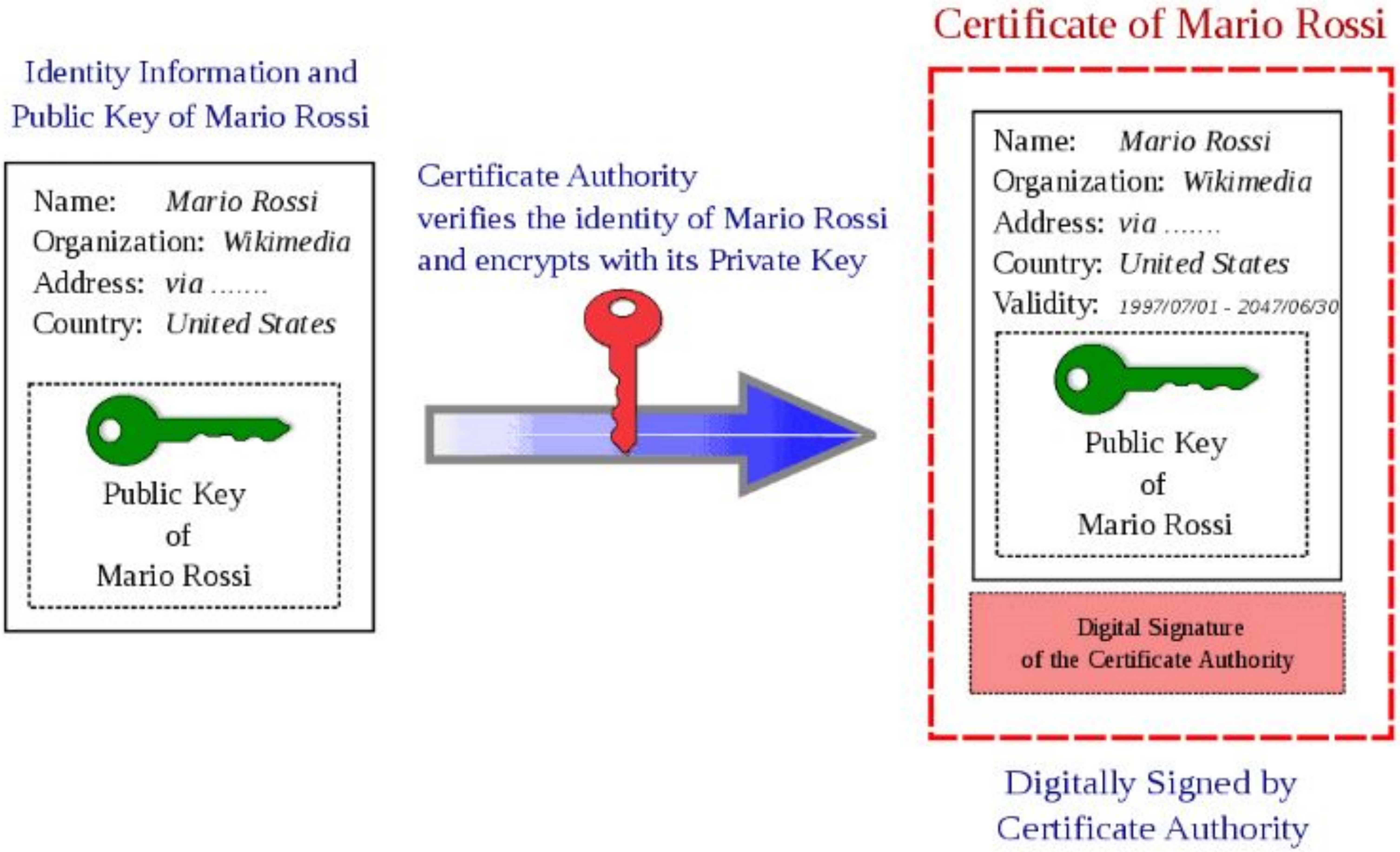
Hash-based message Authentication Code (sha256hmac)

Certificate Authority

A Certfificate Authority (CA) is a trusted organization that issues digital certificates to verify the identity of websites and enable secure ,encrypted communication over the internet.

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


Certificate Authority
Public Key
Certificate
Standard
Certificate
Standard
Banking Website



Identity Information and Public Key of Mario Rossi

Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via* ....
Country: *United States*

Public Key of Mario Rossi

Certificate Authority verifies the identity of Mario Rossi and encrypts with its Private Key

Certificate of Mario Rossi

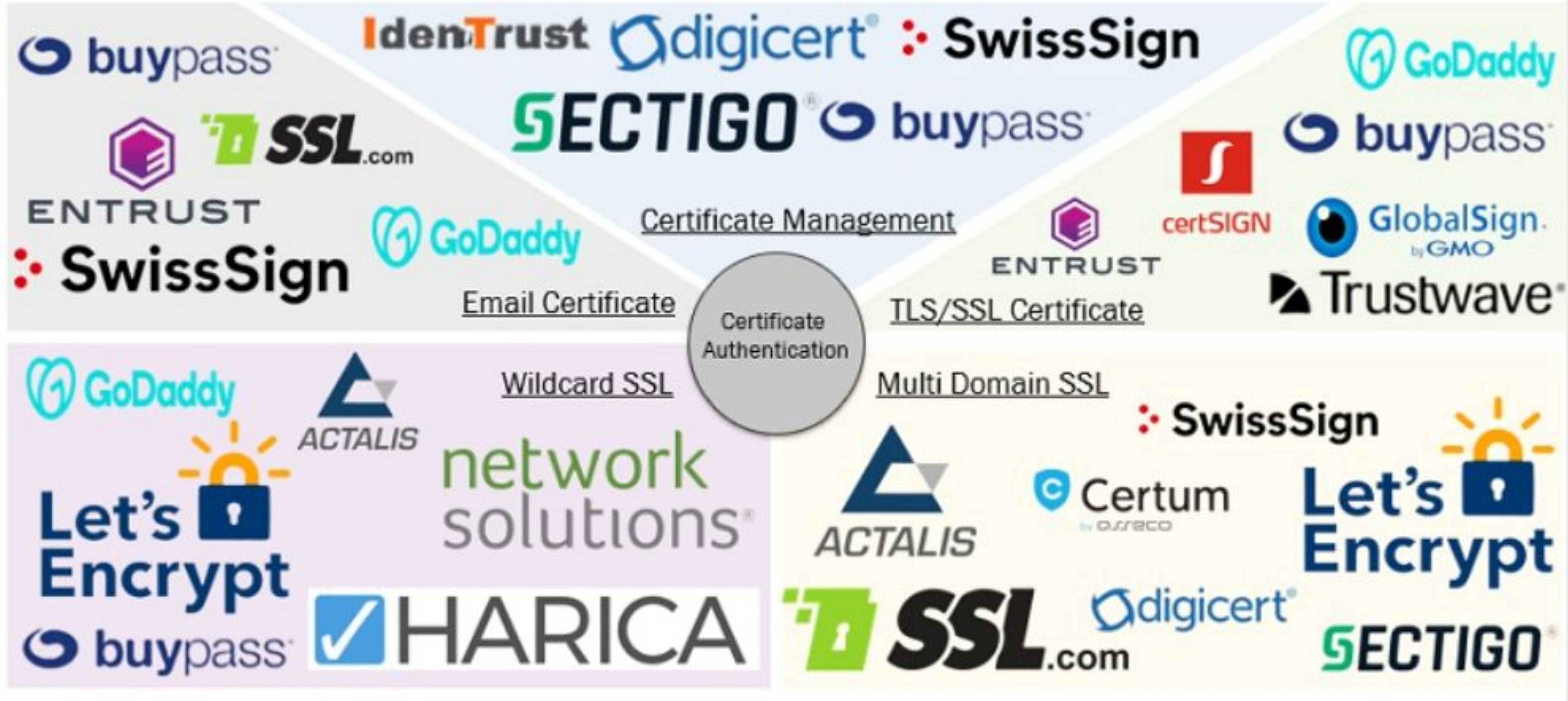
Name: *Mario Rossi*
Organization: *Wikimedia*
Address: *via* ....
Country: *United States*
Validity: *1997/07/01 - 2047/06/30*

Public Key of Mario Rossi

Digital Signature of the Certificate Authority

Digitally Signed by Certificate Authority

Certificate Authority Market Ecosystem



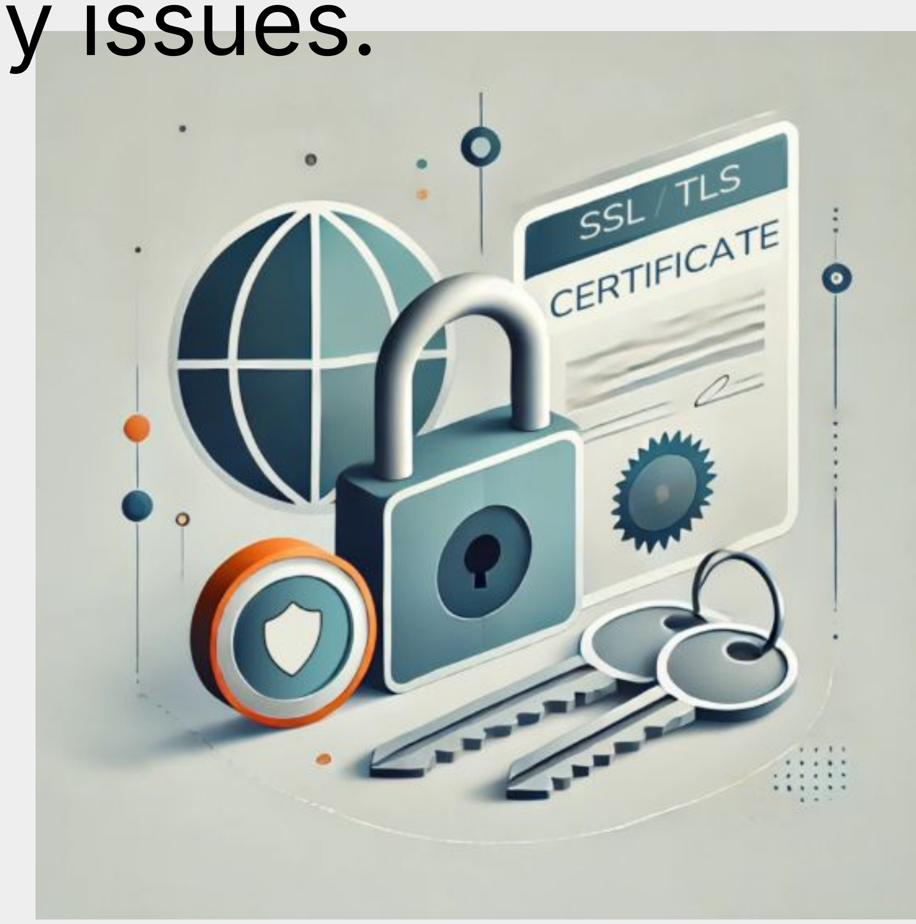
What Is the Difference Between SSL and TLS Certificates?

SSL (Secure Sockets Layer) was the original technology behind security certificates used by websites. SSL certificates were first used in 1995.

Unfortunately, security flaws were found with the original SSL protocol that left it vulnerable to hackers. These vulnerabilities allowed hackers to intercept and modify data as it traveled between the website and the user's browser.

Over the years, several improvements were made to SSL to make it more secure. Here is a quick timeline of the changes as security vulnerabilities were discovered:

SSL 1.0 (unpublished) was never publicly released due to security issues.
SSL 2.0 (1995) was deprecated in 2011 due to security issues.
SSL 3.0 (1996) was deprecated in 2015 due to security issues.
TLS 1.0 (1999) was deprecated in 2021 due to security issues.
TLS 1.1 (2006) was deprecated in 2021 due to security issues.
TLS 1.2 (2008) is still in use.
TLS 1.3 (2018) is still in use.



The SSL protocol is no longer used, but the term SSL certificate stuck, and it is still commonly used as a synonym for TLS certificates.

To summarize, TLS is the evolved form of SSL certificates. Most websites on the internet use TLS certificates. However, they are still commonly referred to as SSL certificates.

Working of TLS

TLS uses a protocol or, we can say, a mechanism known as a client-server handshake mechanism.

It is used to establish a connection that is encrypted and secure to ensure the authenticity of the communication.

Now, whenever a user visits a website at a particular moment, TLS Handshake starts between the client and the web server. Let's see the breakdown of the process in phases:

1.Client Hello :
client: “Hello, i support these SSL/TLS versions and cipher suites...”

2.Server Hello :
server : “hello, i choose this SSL/TLS version and cipher suites...”

3.Server Certificate
Server : “Here is my certificate with my public key .....“

4. Certificate Verification : *(by browser)*
Client : “ i verify your certificate....”

5.Key Exchange :

client : “i encrypt a pre-master secret with your public key ....”
server : “i decrypt the pre master secret with my private key ...”

Benefits of TLS

TLS provides a secure authentication mechanism.

TLS offers special auditing and logging capabilities built directly into the protocol.

TLS controls the data transmitted and received on an encrypted session.

TLS should be used for applications like instant messaging, e-mail, file sharing, audio/video conferencing, and Internet services.

TLS is easy to use as it is implemented beneath the application layer, so most of the operations are invisible to the client (This is what the application layer does).

Conclusion

without TLS ,online banking and shopping would be at high risk, Credit Card numbers , login credential and other sensitive data could be intercepted and read by the attackers. This would lead to Widespeard fraud and financial loss.

It is essential for the data to be encrypted and also without TLS Email would not be a secure method of communication , email sent over the network could be intercepted and read by the attackers

Without TLS, there is no way to ensure whether you are interacting with a legitimate website rather than a phising site set up to steal your personal information.

Conclusion
:

So Next time , you are browsing the web or sending an email ,

Think of TLS as your own Personal bodyguard Keeping you safe and secure in the digital world .

Q&A

Thank You