Section 1.1.3 Computer Networks Fundamentals

HTTPS

{Hypertext Transfer Protocol Secure}

Cracking OSCP: Your Roadmap to Ethical Hacking Success

YouTube: HackProKP – Kailash Parshad

Socials: HackProKP

Github: https://github.com/at0m-b0mb/Cracking-OSCP-Your-Roadmap-to-Ethical-Hacking-Success

Complete Youtube Playlist:
https://www.youtube.com/watch?v=MvkNbn8i2so&list=PLyrv3TPh3ejYNZipa0OIUvkdjHeUTRJ3J&index=1&t=0s

WHAT IS HTTPS?

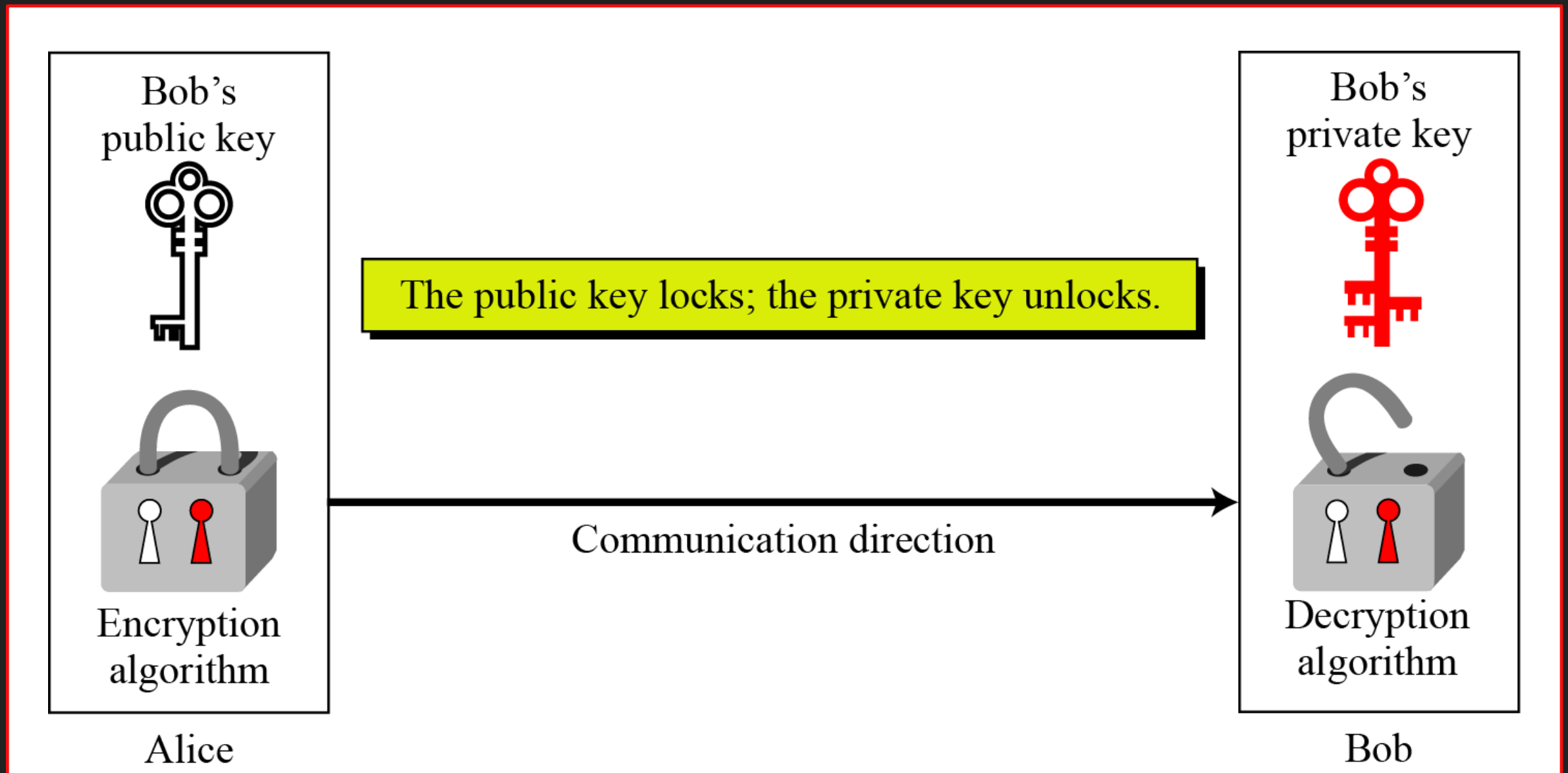
- HTTPS, or **Hypertext Transfer Protocol Secure**, is an extension of HTTP (**Hypertext Transfer Protocol**) designed to provide a secure communication channel over the Internet. It is widely used to ensure the **confidentiality** and **integrity** of data exchanged between a user's web browser and a website

Encryption?

- **SSL/TLS Protocols**: HTTPS relies on SSL (**Secure Sockets Layer**) or its successor, TLS (**Transport Layer Security**), to encrypt data. These protocols ensure that the information exchanged between the user's browser and the server is secure.

Encryption?

- **Public Key Cryptography**: HTTPS uses public key cryptography to secure communication. The server has a **public key** and a **private key**. The public key is used for encryption, and the private key is **kept secret** and used for decryption. This **asymmetrical encryption** ensures that even if someone intercepts the communication, they cannot easily decipher it without the private key.


Bob's public key
Encryption algorithm
Alice
The public key locks; the private key unlocks.
Communication direction
Bob's private key
Decryption algorithm
Bob

Actual Public Key of my Website 😎

Certificate


```
-----BEGIN CERTIFICATE-----
MIIFjzCCBHegAwIBAgIQQkw9VbaG9skTfbM2z+EKszANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFN1cnZpY2VzIExM
QzETMBEGA1UEAxMKR1RTIENBIDFQNTAeFw0yNDAxMjAwMzU2NDZaFw0yNDA0MTkw
MzU2NDVaMCMxITAfBgNVBAMTGGF0MG0tYjBtYi5ncmVhdC1zaXRlLm51dDCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPW/C3gnmihmUQezfJuAf3RPLsrg
LLjgi4CBDcCvVfW+iaQnKglEW01kZHo0u1bosZMwdgkfRmt/qik9ZKfyZ7ZQixoM
yVGGJQV0txrcX056N1yiy4QTJa7JnJty1uX+yWSdYz78CCq72C304tv1YASXGT21
E28xB6x1lLkZ1S5APNH6FP4qWqS4lkwnBQZwdRfpRuWD/4RjU4hs94njc8LIf3it
NHb31VqnW10hJKdiMnnPemFPrbZ9TZ7BHoCsilorAIntwm8ah29exeZ7K/dvizjk
OQbboie+SADlbnzKqeTKjFxGII3uJilFuewEmQNvU1xYQ5k7gcx/biFVEisCAwEA
AaOCApowggKWMA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcDATAM
BgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTiTGQDE8ywQDgB0FRrakGVHaXdgzAfBgNV
HSMEGDAWgBTV/J4N3x7K3QiX124rxV/FK/XsuDB4BggrBgEFBQcBAQRsMGowNQYI
KwYBBQUHMAGGKWh0dHA6Ly9vY3NwLnBraS5nb29nL3MvZ3RzMXA1Lz1GSWtoZi16
MGR3MDEGCCsGAQUFBzAChiVodHRwOi8vcGtpLmdvb2cvcmVwby9jZXJ0cy9ndHMx
cDUuZGVyMD8GA1UdEQQ4MDaCGGF0MG0tYjBtYi5ncmVhdC1zaXRlLm51dIIaKi5h
dDBtLWIwbWIuZ3JlYXQtc2l0ZS5uZXQwIQYDVR0gBBowGDAIBgZngQwBAgEwDAYK
KwYBBAHWeQIFAzA8BgNVHR8ENTAzMDGgL6AthitodHRwOi8vY3Jscy5wa2kuZ29v
Zy9ndHMxcDUvWmVHW1lvYTNmNnMuY3JsMIIBAwYKKwYBBAHWeQIEAgSB9ASB8QDv
AHYA7s3QZNXbGs7FXLedtM0TojKHRny87N7DUUhZRnEftZsAAAGNJTp/YQAABAMA
RzBFAiEAxd/Kz5OFqbiZ49tX09XNCZtLcBwx+nyqBUdn9C21yjUCICv2jSk2N6pz
fcMX588DafbT5244giLvzm7TH90s3hHFAHUASLDja9qmRzQP5WoC+p0w6xxSActW
3SyB2bu/qznYhHMAAAGNJTp/gwAABAMARjBEAiA1HHPNx9g7A8k7/GHhNH7cr4Jd
nQ+zhksgNRp5MNpEmwIgIn0KvL/Ot1OPNDJ7w6aap5SJKYxaVw9Xpz2RMFE4cQkw
DQYJKoZIhvcNAQELBQADggEBADzdNxcC3QVpK/Lw/jKSWdFrJpQNmb5MPu9VKvyf
87JffFCNIoBl/LTy5LskV1sxB5wQZClo1AzooWeVD1rHHjWjRDAz8s6eN10bkF7m
mjVuBxdQe05ZEhd+p4AL83wUzvFLS97XP9uLSLu62W0a2PRfowmAbQ9WK7Why+6c
kPm/hpbyynqiTQTu8WGmcnEpbx39TCtkxabQEVOuk7XPvoIacwN3UQqptFiir815
JJupL2S4wd1RMEbNGA9UQHDziKPOpxuQnJ4JvmHc6nkv983JkmoFoKbEJTbSdYRV
WFJj0Ye6TYXfk1CBwsmFBnPn1Yh+rtvHROvpfjPSrMn0TgI=
-----END CERTIFICATE-----
```

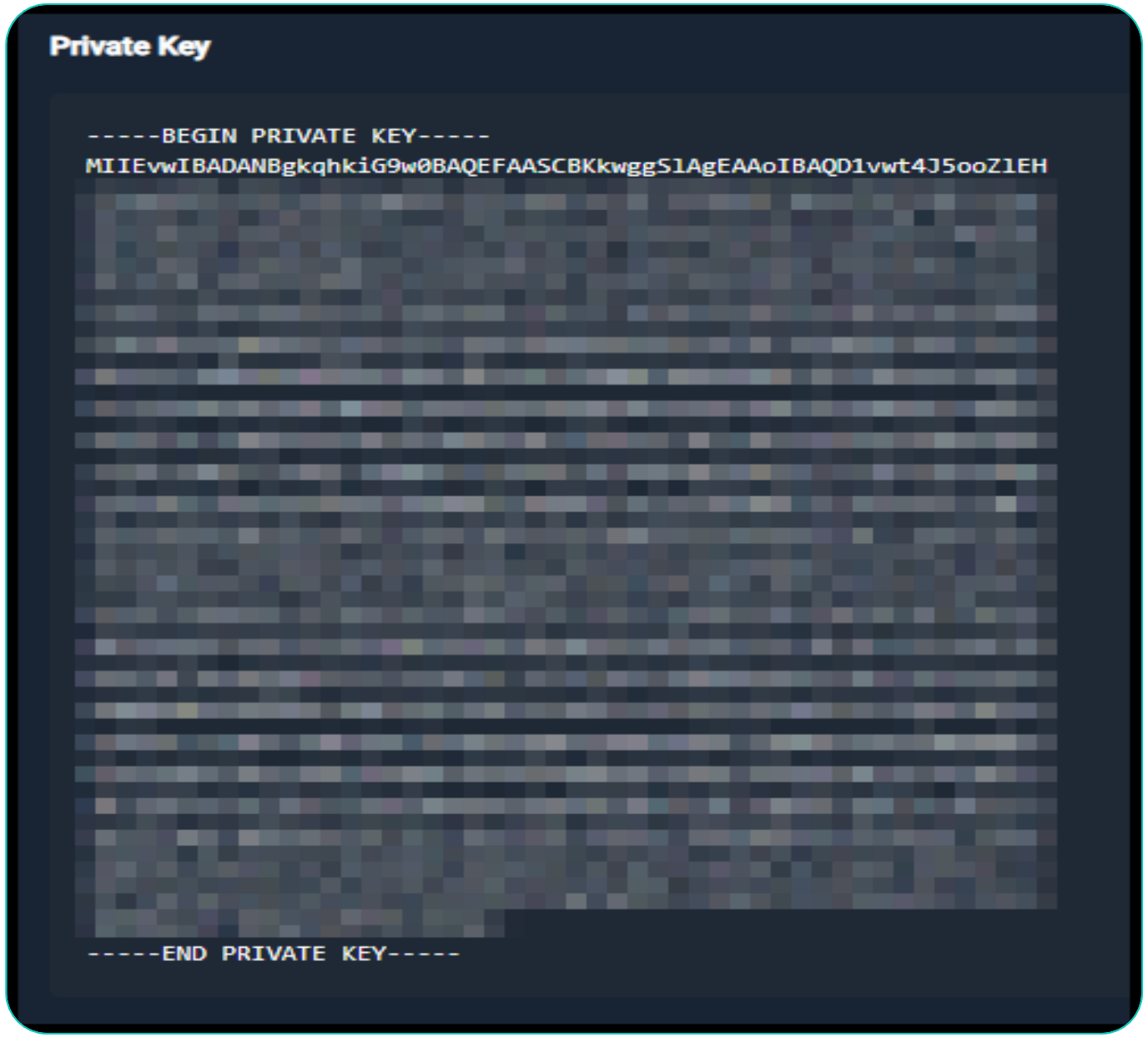

Public Key

Distribution: The public key is freely distributed and known by anyone who wants to communicate securely with the entity associated with that public key.

Encryption: When someone wants to send a secure message to the owner of the public key, they use it to encrypt the message

Authentication: Public keys are also used for authentication. Decrypting a message with the private key associated with a public key confirms its origin from the corresponding entity.

Private Key of my Website? 🔐



Private Key

Secrecy: The private key must be kept confidential and only known to the entity to which it belongs. It should never be shared with others.

Decryption: The private key is used to decrypt messages that were encrypted with the corresponding public key. Only the entity possessing the private key can decrypt these messages.

Digital Signatures: Private keys are also used to create digital signatures. A digital signature is a cryptographic way of proving the origin and integrity of a message or document.

Key Pair Relationship

- **Mathematical Relationship**: The public and private keys in a key pair are mathematically related, but it is computationally infeasible to derive one key from the other. This relationship forms the basis of the security provided by public key cryptography.
- **Key Generation:** When a user or system generates a key pair, the public and private keys are generated together in such a way that information encrypted with one key can only be decrypted with the other.

Use Cases:

- **Secure Communication:** Public key cryptography is commonly used for secure communication over untrusted networks, such as the internet. It ensures that only the intended recipient can decrypt and read the message.

Use Cases:

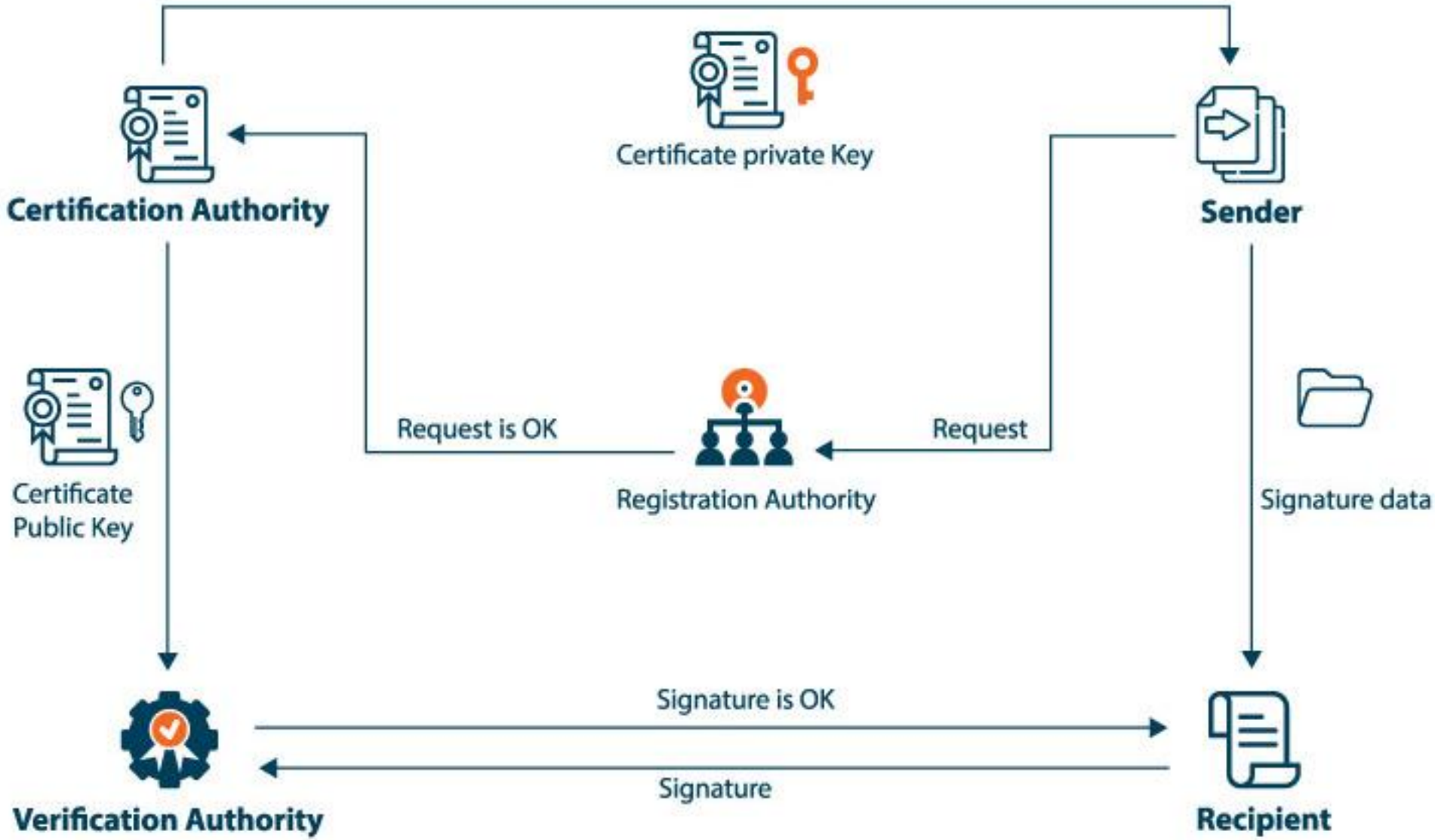
- **Digital Signatures:** Digital signatures verify the authenticity and integrity of a message, providing a way to ensure that a message has not been tampered with and was indeed sent by the claimed sender.

Use Cases:

- **Key Exchange:** Public key cryptography is also used in key exchange protocols, such as the Diffie-Hellman key exchange, to establish a shared secret key between two parties without needing a secure pre-existing channel.

Key Management:

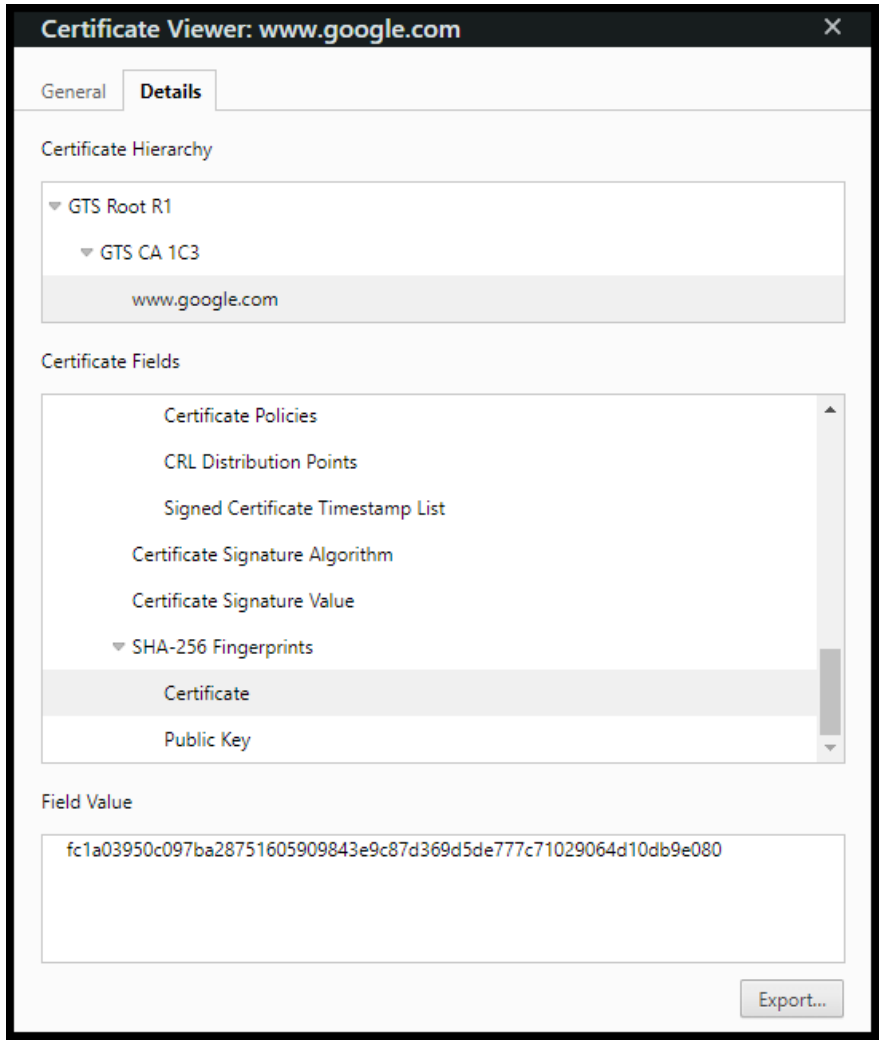
- **Secure Storage:** Private keys must be securely stored to prevent unauthorized access. This is crucial because anyone with the private key can decrypt messages or forge digital signatures.
- **Certificate Authorities (CAs):** In the context of SSL/TLS certificates, a Certificate Authority verifies the identity of an entity and issues a certificate containing the entity's public key. This helps users trust the authenticity of a public key.

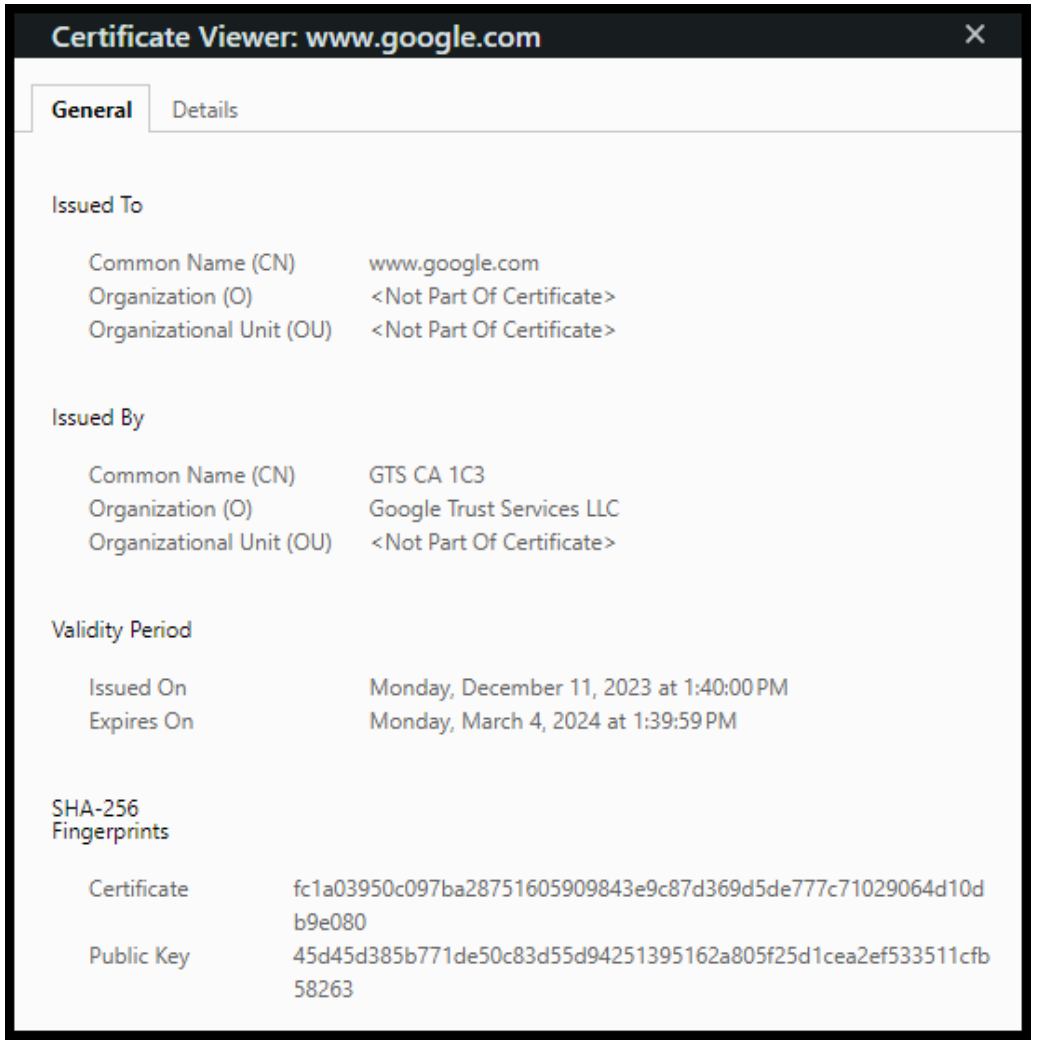


https://cheapsslweb.com/blog/what-is-a-certificate-authority-in-pki

Certificate Authority

- A Certificate Authority **(CA)** is a trusted entity responsible for issuing digital certificates in public key infrastructure. CAs verify the authenticity of certificate requests using various methods, such as domain ownership confirmation, legal entity validation, or other agreed-upon processes. Once satisfied, the CA issues a digital certificate, including a public key, which is used to establish secure communication and assure users of a website's legitimacy.

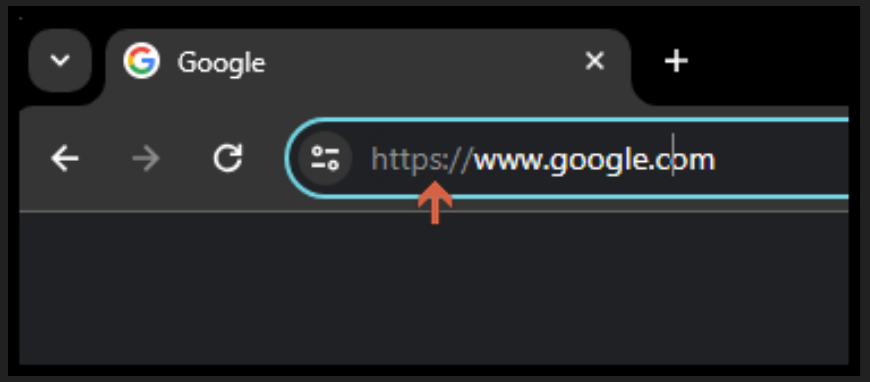

Certificate Viewer: www.google.com
General
Details
Certificate Hierarchy
GTS Root R1
GTS CA 1C3
www.google.com
Certificate Fields
Certificate Policies
CRL Distribution Points
Signed Certificate Timestamp List
Certificate Signature Algorithm
Certificate Signature Value
SHA-256 Fingerprints
Certificate
Public Key
Field Value
fc1a03950c097ba28751605909843e9c87d369d5de777c71029064d10db9e080
Export...


Certificate Viewer: www.google.com
General
Details
Issued To
Common Name (CN) www.google.com
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) GTS CA 1C3
Organization (O) Google Trust Services LLC
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Monday, December 11, 2023 at 1:40:00 PM
Expires On Monday, March 4, 2024 at 1:39:59 PM
SHA-256 Fingerprints
Certificate fc1a03950c097ba28751605909843e9c87d369d5de777c71029064d10db9e080
Public Key 45d45d385b771de50c83d55d94251395162a805f25d1cea2ef533511cfb58263

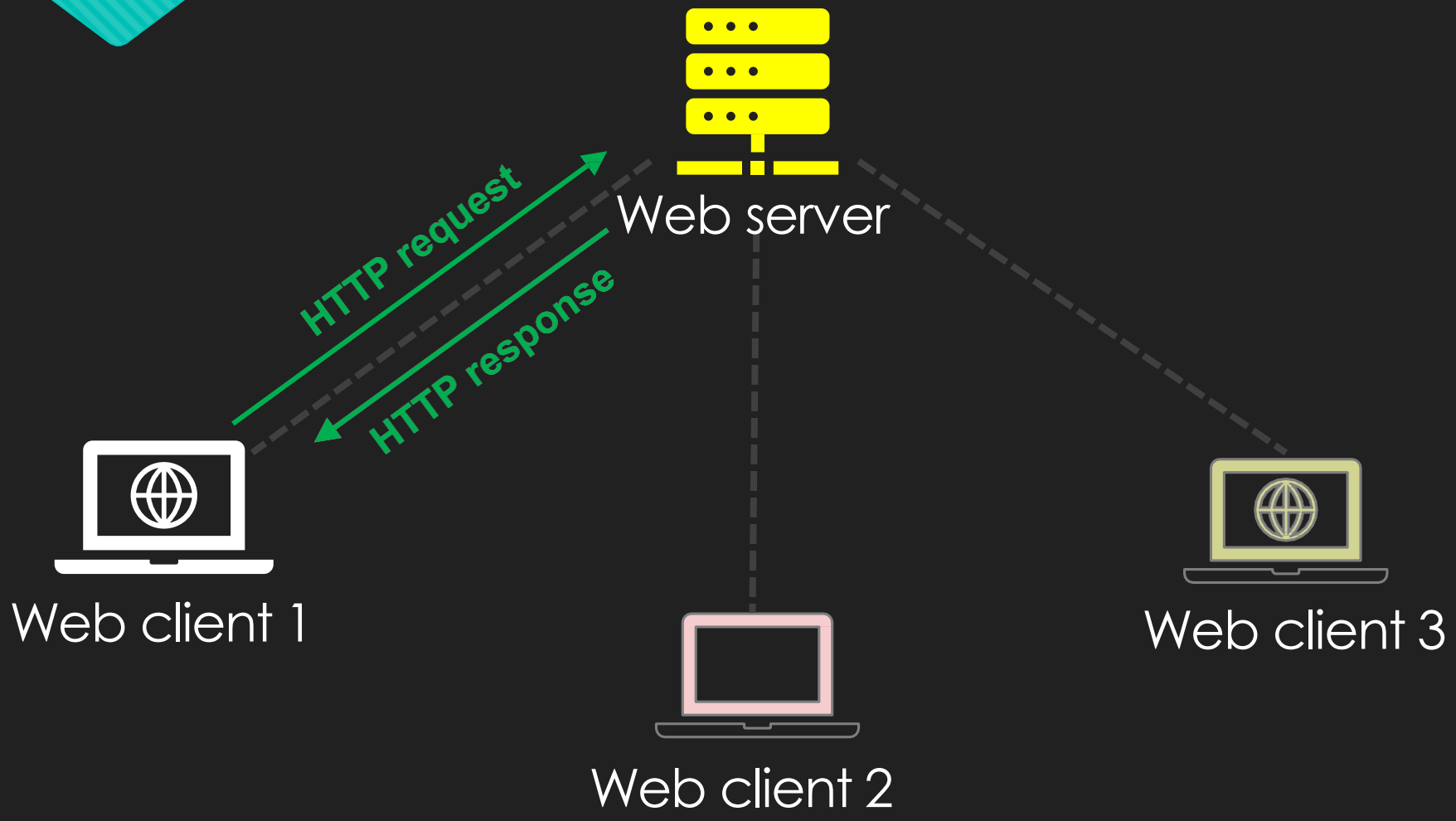
URL (Uniform Resource Locator):

http://www.abc.com/path/test.txt

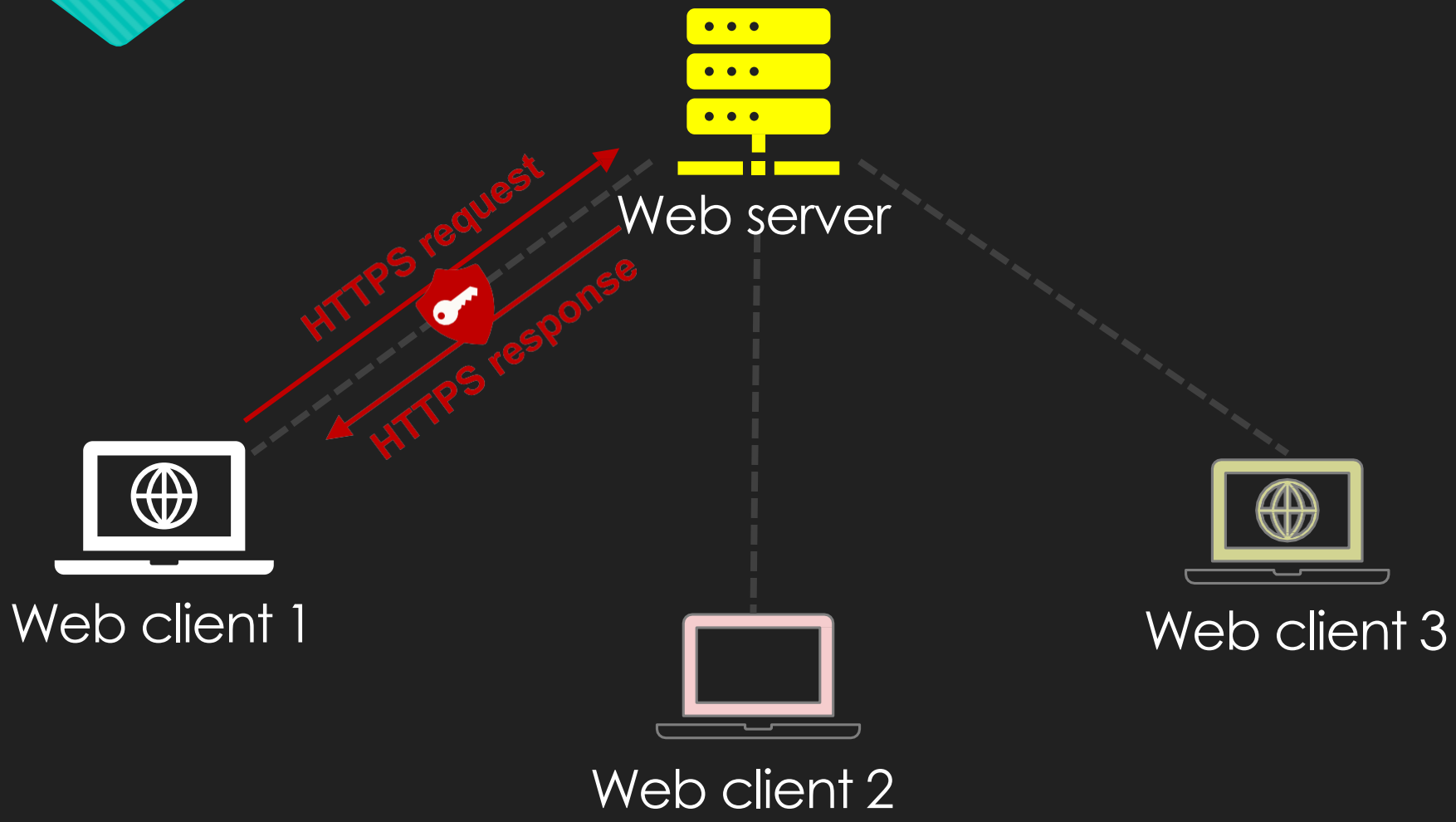
https://www.abc.com/path/test.txt



HOW DOES IT WORK? HTTP!



HOW DOES IT WORK? HTTPS!



Thank You!

😊 ❤️

Please Like 👍 and Subscribe 📖 to never miss a video 🎥

And to help me with the Algorithm 🤖

And It's completely Free!!! 💵

Love you guys ❤️