

# CyberShark 3001 – The project and the lessons

**Ross Bagurdes**

IT Educator and Engineer  
NetworkNerd.guru



# Ross Bagurdes

<https://networknerd.guru>

Author of more than 100 hours of IT training in Network +, CCNA, Wireshark, Firewalls, and more.

[www.pluralsight.com](http://www.pluralsight.com)

[ross@networknerd.guru](mailto:ross@networknerd.guru)



@NetworkNerdRoss



@Bagurdes



# The Idea



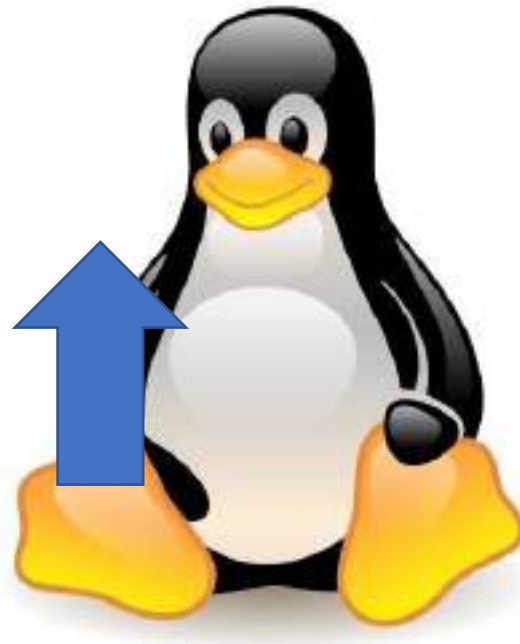
# The Idea





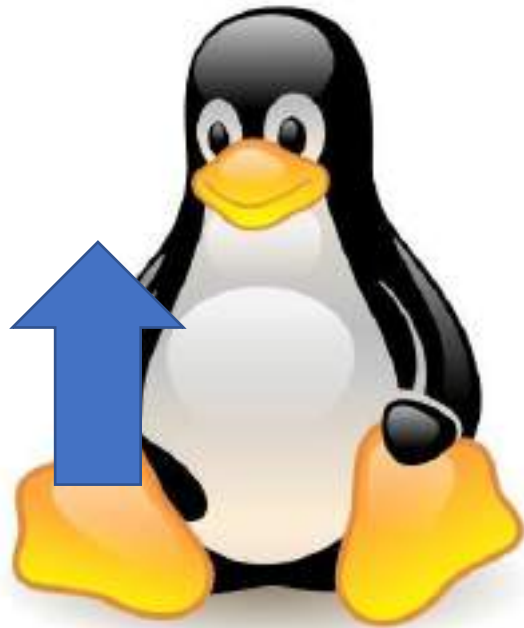


# Goals



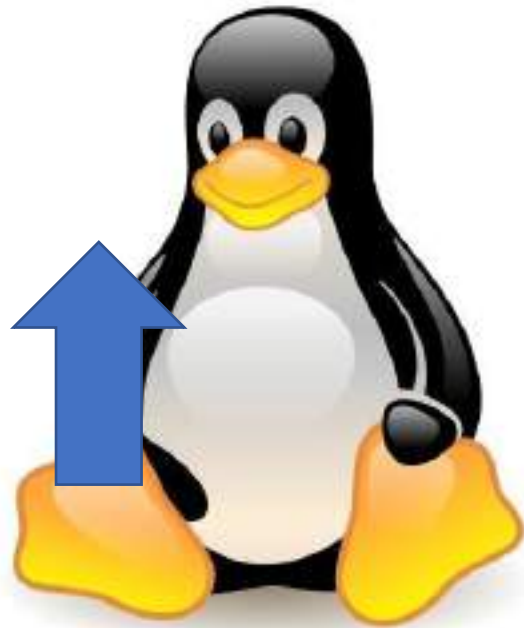


# Goals





# Goals



# The Design



**the Tubes**

# The Design



**Magic Box**



**the Tubes**



# The Design



**Magic Box**



**the Tubes**



# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics





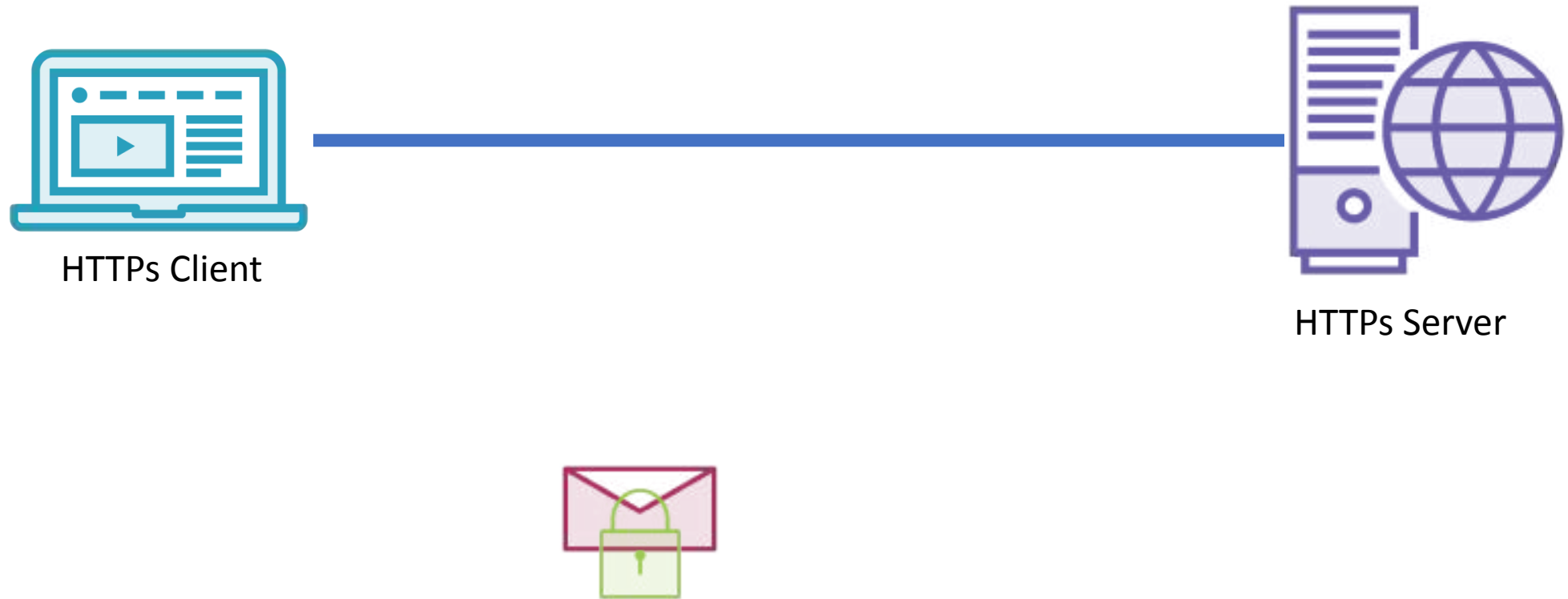
# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics

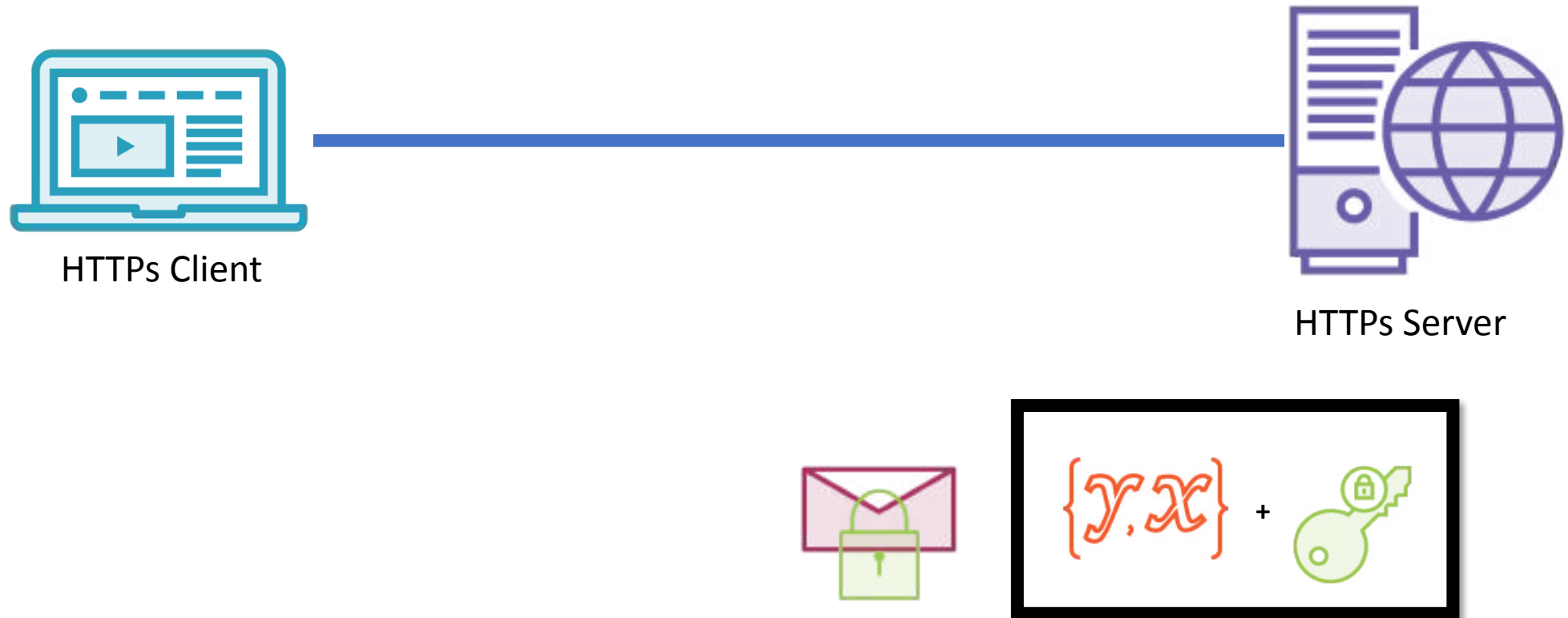




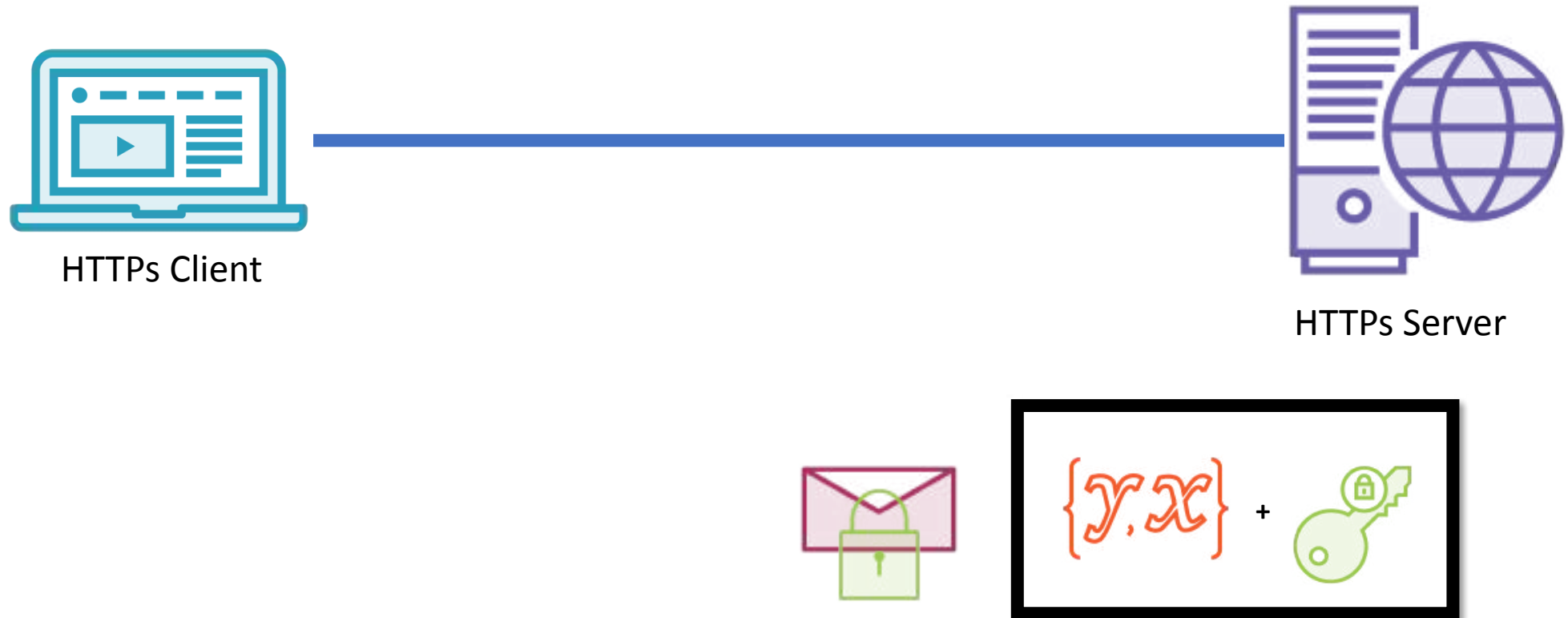
# Data Encryption Basics



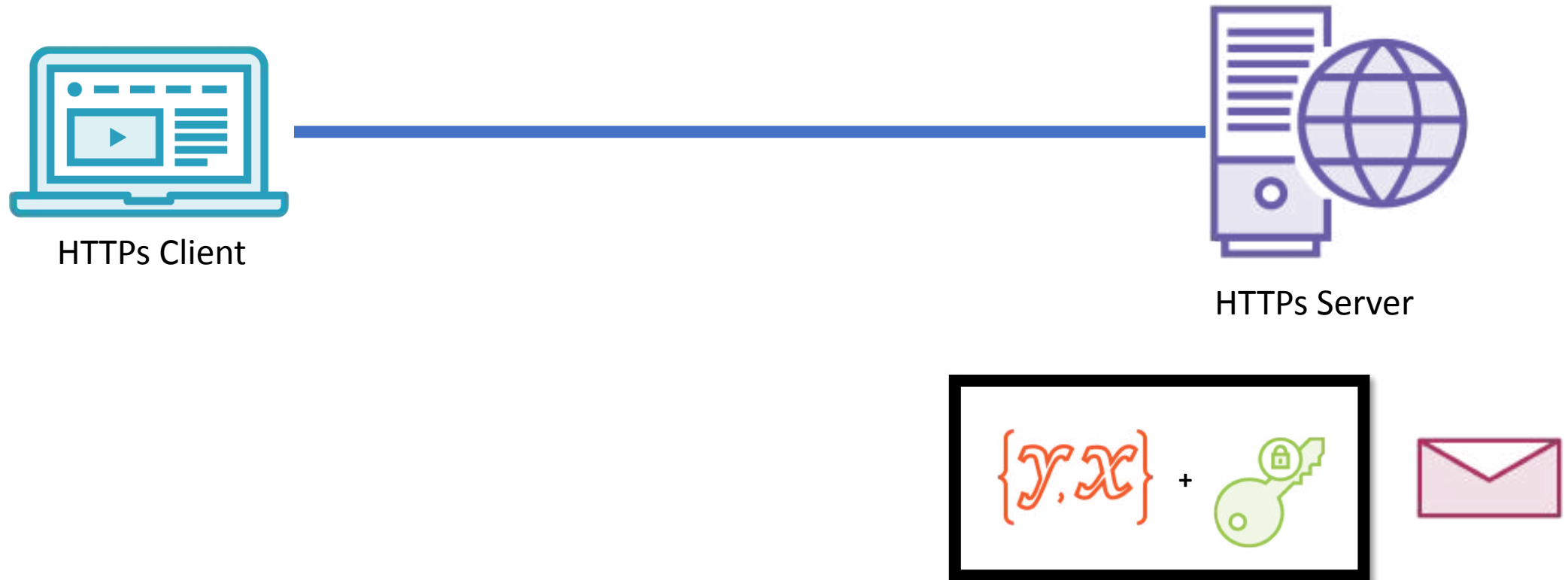
# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics





# Data Encryption Basics



# Data Encryption Basics



# Data Encryption Basics



HTTPs Client



HTTPs Server



# Data Encryption Basics



# Data Encryption Basics

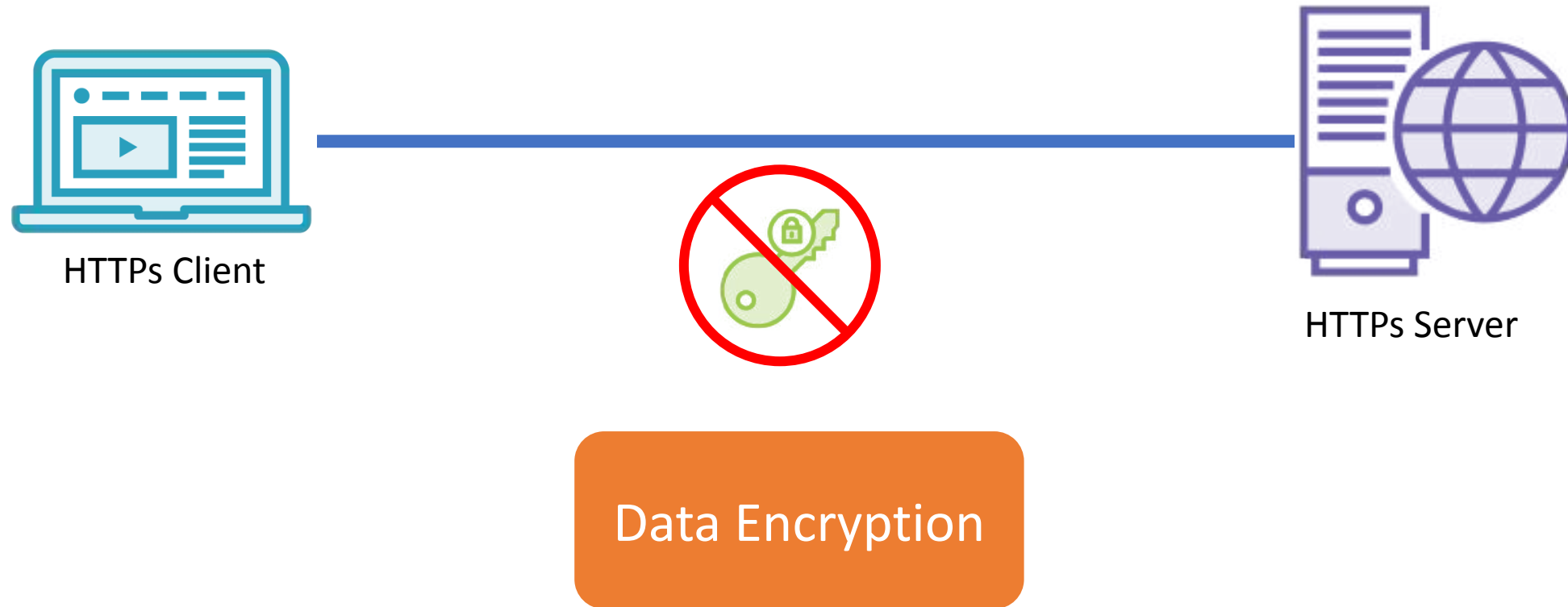




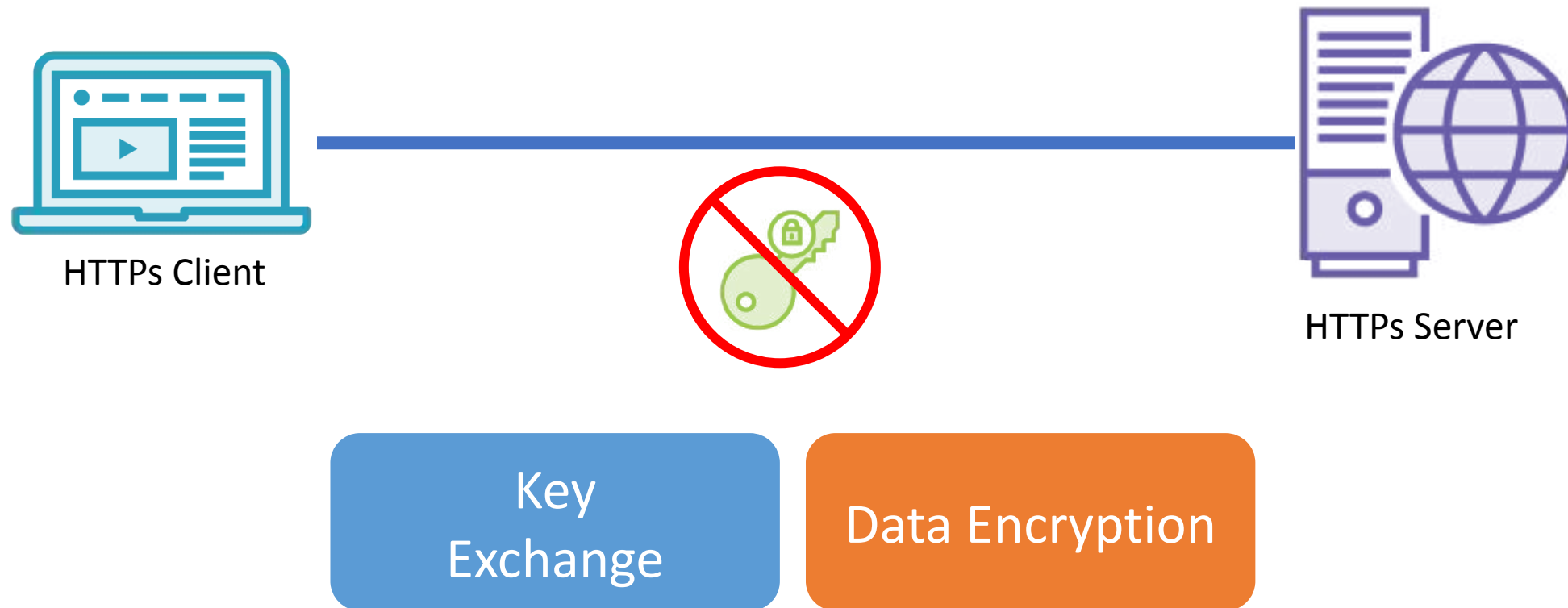
# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



Rivest Shamir Adleman  
(RSA) 1977



# Exchanging the Secret Key



Rivest Shamir Adleman  
(RSA) 1977

Diffie-Hellman (and Merkle)  
(DH) 1976

# Exchanging the Secret Key



HTTPs Client



HTTPs Server

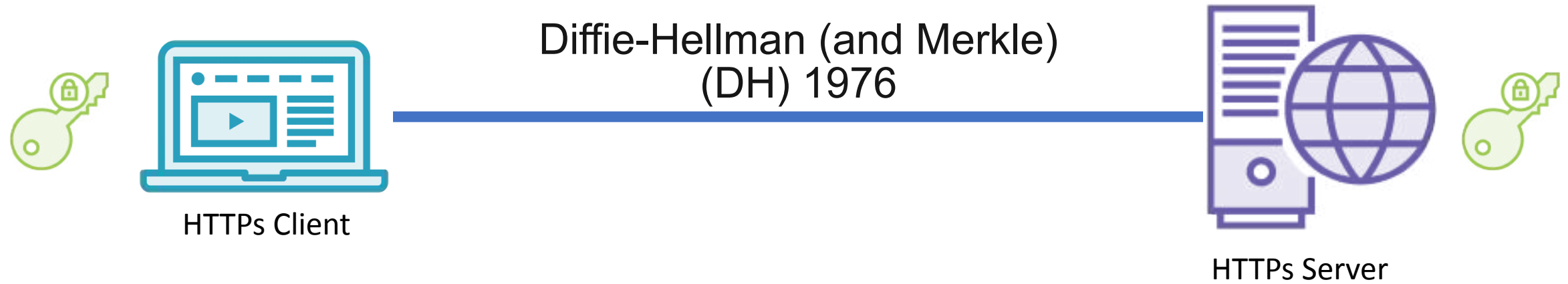


Rivest Shamir Adleman  
(RSA) 1977

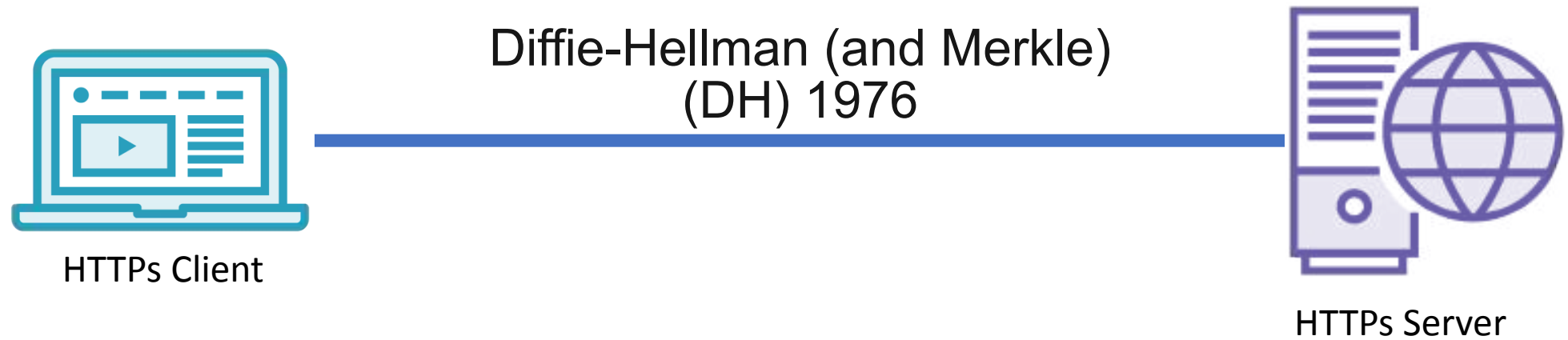
Diffie-Hellman (and Merkle)  
(DH) 1976


Elliptical Curve Diffie  
Hellman Ephemeral  
(ECDHE) 2011

# Exchanging the Secret Key

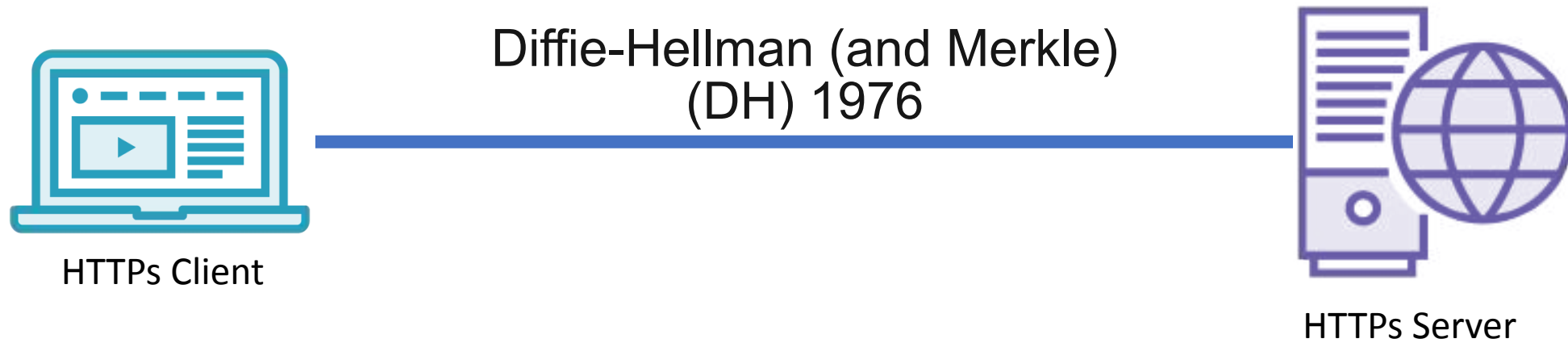


# Exchanging the Secret Key



$$p = 149$$
$$g = 17$$


# Exchanging the Secret Key

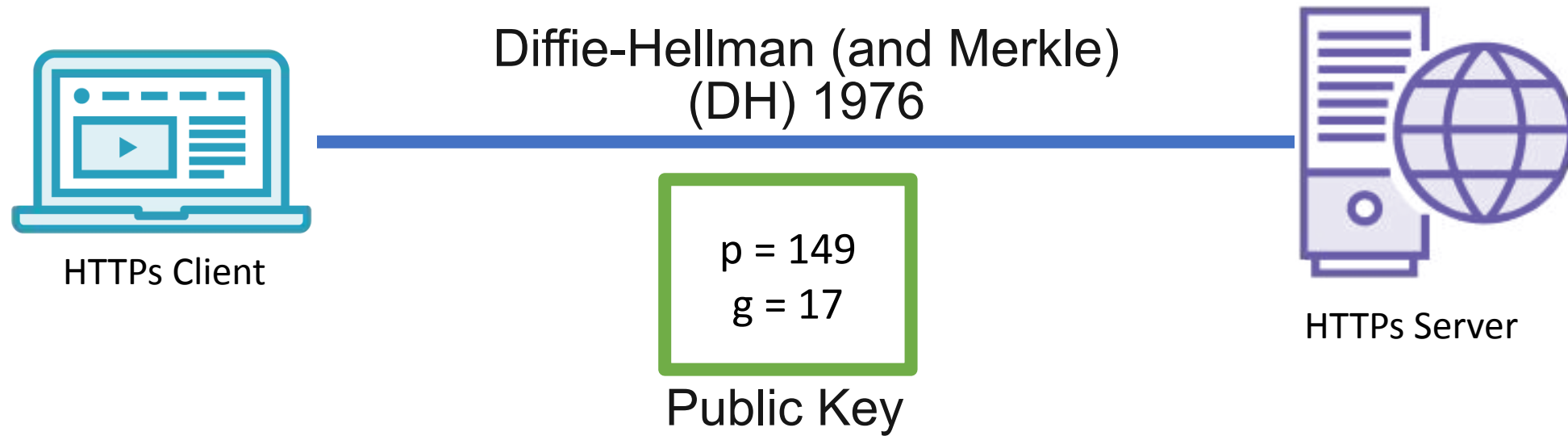


$p = 149$   
 $g = 17$

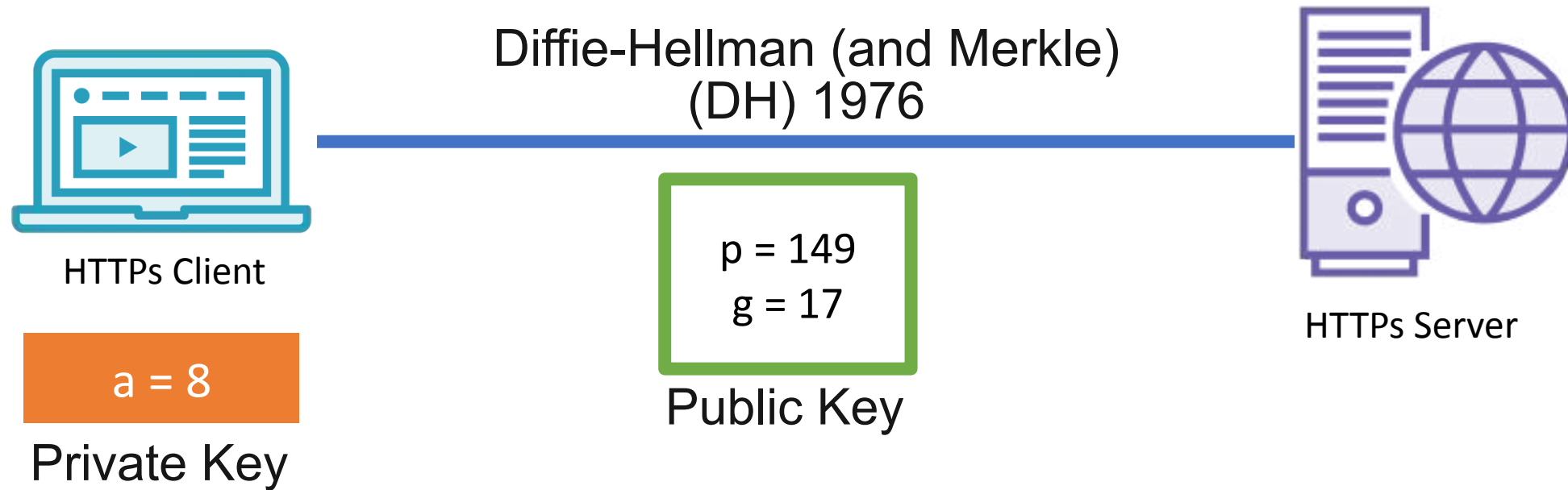




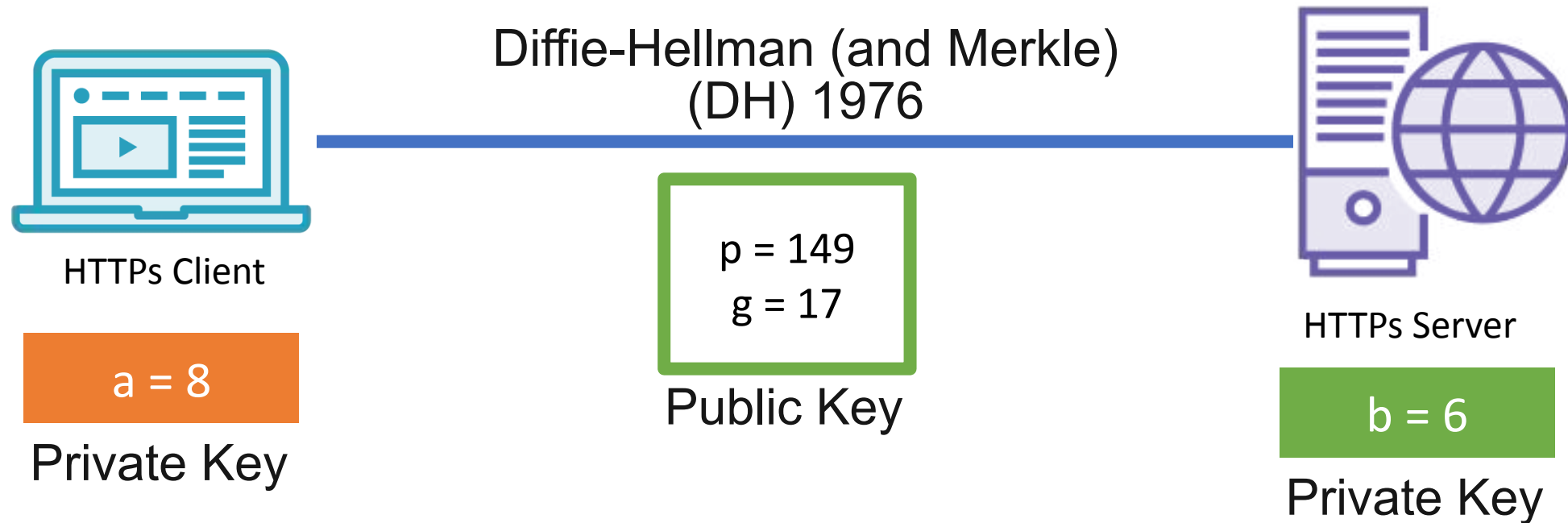
# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



$a = 8$

$b = 6$

# Exchanging the Secret Key

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^a \text{ MOD } p = \text{Key Share}(a)$

$g^b \text{ MOD } p = \text{Key Share}(b)$

$a = 8$

$b = 6$

# Exchanging the Secret Key

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

$g^a \text{ MOD } p = \text{Key Share}(a)$

$a = 8$

$b = 6$

# Exchanging the Secret Key

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



Private Key

HTTPs Server

$g^b \text{ MOD } p = \text{Key Share}(b)$

$17^8 \text{ MOD } p = \text{Key Share}(a)$



# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

$17^8 \text{ MOD } p = \text{Key Share}(a)$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

$17^8 \text{ MOD } 149 = \text{Key Share}(a)$

# Quick Math Lesson

95 divided by 8

95 divided by 8

$$\frac{95}{8}$$

95 divided by 8

$$\begin{array}{r} 8 \overline{) 95} \end{array}$$

$$8 \overline{) 95}$$



$$\begin{array}{r} 1 \\ 8 \overline{) 95} \end{array}$$

$$\begin{array}{r} 1 \\ 8 \overline{) 95} \\ \underline{8} \end{array}$$

$$\begin{array}{r} 1 \\ 8 \overline{) 95} \\ \underline{8} \\ 1 \end{array}$$

$$\begin{array}{r} 1 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \end{array}$$

$$\begin{array}{r} 1 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \end{array}$$

$$\begin{array}{r} 11 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \end{array}$$

$$\begin{array}{r} 11 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \end{array}$$



$$\begin{array}{r} 11 \\ \hline 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \\ 7 \end{array}$$

$$\begin{array}{r} 11.\text{xxxx} \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \\ 7 \end{array}$$

$$\begin{array}{r} 11r7 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \\ 7 \end{array}$$

$$\begin{array}{r} 11r7 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \\ 7 \end{array}$$

$$\begin{array}{r} 11r7 \\ 8 \overline{) 95} \\ \underline{8} \\ 15 \\ \underline{8} \\ 7 \end{array}$$

11 r 7

r 7



95 mod 8

Modulus 7

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

$17^8 \text{ MOD } 149 = \text{Key Share}(a)$

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

$17^8 \text{ MOD } 149 = \text{Key Share}(a)$

$5 = \text{Key Share}(a)$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

5

Key  
Share(a)

$g^b \text{ MOD } p = \text{Key Share}(b)$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

5

Key  
Share(a)

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

$g^b \text{ MOD } p = \text{Key Share}(b)$

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

5

Key  
Share(a)

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

$b = 6$

Private Key

$$17^6 \text{ MOD } 149 = \text{Key Share}(b)$$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

Private Key

5

Key  
Share(a)

$$17^6 \text{ MOD } 149 = \text{Key Share}(b)$$

$$16 = \text{Key Share}(b)$$

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

5

Key  
Share(a)

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

16

Key  
Share(b)

$b = 6$

Private Key



# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

5

Key  
Share(a)

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

16

Key  
Share(b)

$b = 6$

Private Key

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

16

Key  
Share(b)

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

5

Key  
Share(a)

$b = 6$

Private Key

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key



HTTPs Client

16

Key  
Share(b)

$\text{Key Share}(b)^a \text{ MOD } p = \text{Key}$

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

5

Key  
Share(a)

$\text{Key Share}(a)^b \text{ MOD } p = \text{Key}$

Private Key

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key

Private Key



HTTPs Client



HTTPs Server

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

16

Key  
Share(b)

5

Key  
Share(a)

Key Share(b)<sup>a</sup> MOD p = Key

$$16^8 \text{ MOD } 149 = \text{Key}$$

Key Share(a)<sup>b</sup> MOD p = Key

$$5^6 \text{ MOD } 149 = \text{Key}$$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key

Private Key



HTTPs Client



HTTPs Server

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

16

Key  
Share(b)

5

Key  
Share(a)

Key Share(b)<sup>a</sup> MOD p = Key

$16^8 \text{ MOD } 149 = \text{Key}$

129

Key Share(a)<sup>b</sup> MOD p = Key

$5^6 \text{ MOD } 149 = \text{Key}$

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key

Private Key



HTTPs Client



HTTPs Server

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

16

Key  
Share(b)

5

Key  
Share(a)

Key Share(b)<sup>a</sup> MOD p = Key

$16^8 \text{ MOD } 149 = \text{Key}$

129

Key Share(a)<sup>b</sup> MOD p = Key

$5^6 \text{ MOD } 149 = \text{Key}$

129

# Exchanging the Secret Key

$a = 8$

$b = 6$

Private Key

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976



HTTPs Server

16

Key  
Share(b)

5

Key  
Share(a)

Key Share(b)<sup>a</sup> MOD p = Key

Key Share(a)<sup>b</sup> MOD p = Key

$16^8 \text{ MOD } 149 = \text{Key}$

$5^6 \text{ MOD } 149 = \text{Key}$

129



129



$a = 8$

$b = 6$

# Exchanging the Secret Key

Private Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976



Private Key



# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976



# TLS Key Exchange Protocols

# Data Encryption

Key  
Exchange

Data Encryption

# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

RSA

Diffie Hellman

Elliptical Curve  
Diffie Hellman

# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

~~RSA~~

Diffie Hellman

Elliptical Curve  
Diffie Hellman

# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

~~RSA~~

~~Diffie Hellman~~

Elliptical Curve  
Diffie Hellman



# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

~~RSA~~

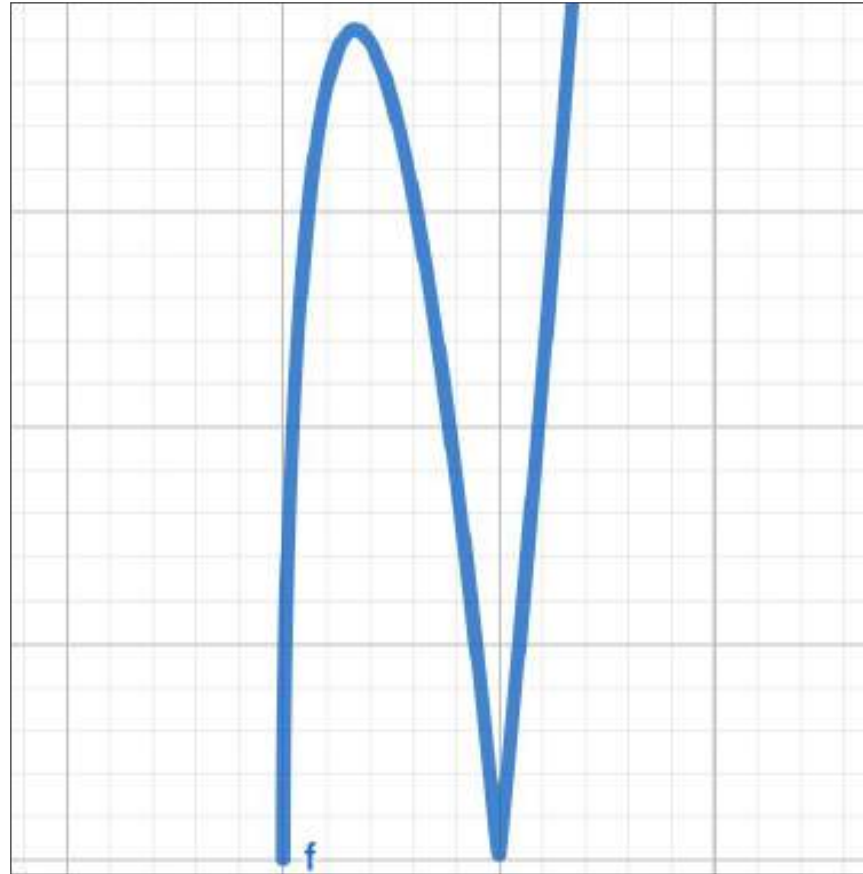
~~Diffie Hellman~~

Elliptical Curve  
Diffie Hellman

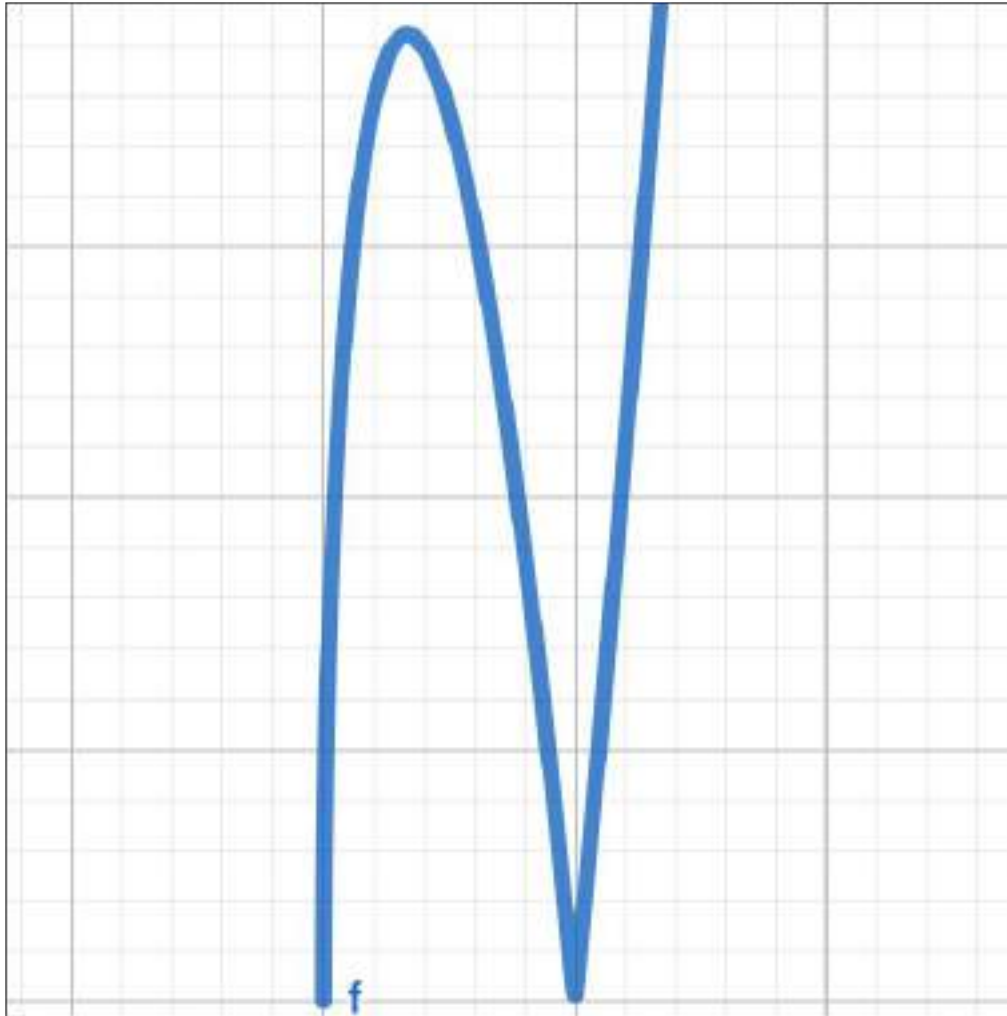
Elliptical Curve  
Diffie Hellman

# Elliptical Curve Diffie Hellman

# Elliptical Curve



# Elliptical Curve



## Curve Types

---

x25519

secp256r1

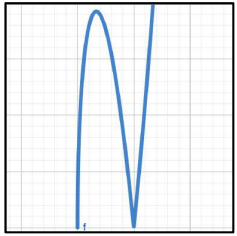
secp284r1

fecp521r1

ffdhe2048

ffdhe3073

# TLS 1.3 ECDHE Key Exchange

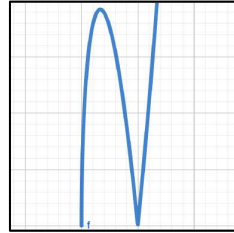


HTTPs Client



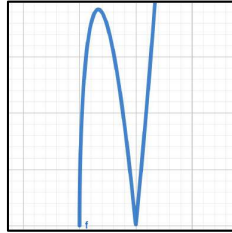
HTTPs Server

# TLS 1.3 ECDHE Key Exchange



HTTPs Client

# TLS 1.3 ECDHE Key Exchange

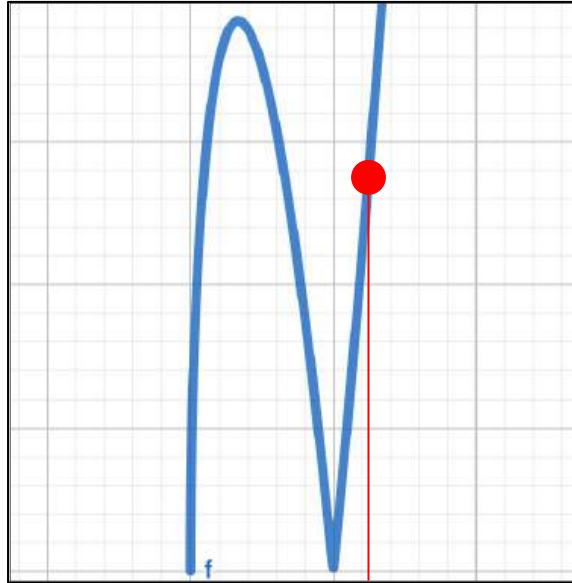


HTTPs Client

Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

# TLS 1.3 ECDHE Key Exchange



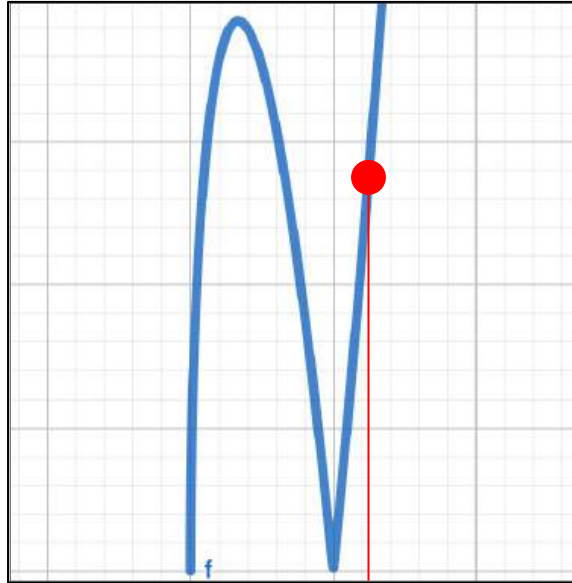
Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

<https://curves.xargs.org>



# TLS 1.3 ECDHE Key Exchange

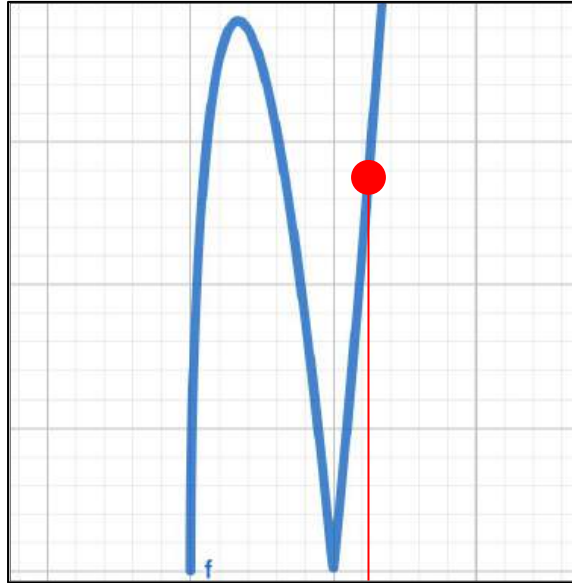


Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

<https://curves.xargs.org>

# TLS 1.3 ECDHE Key Exchange



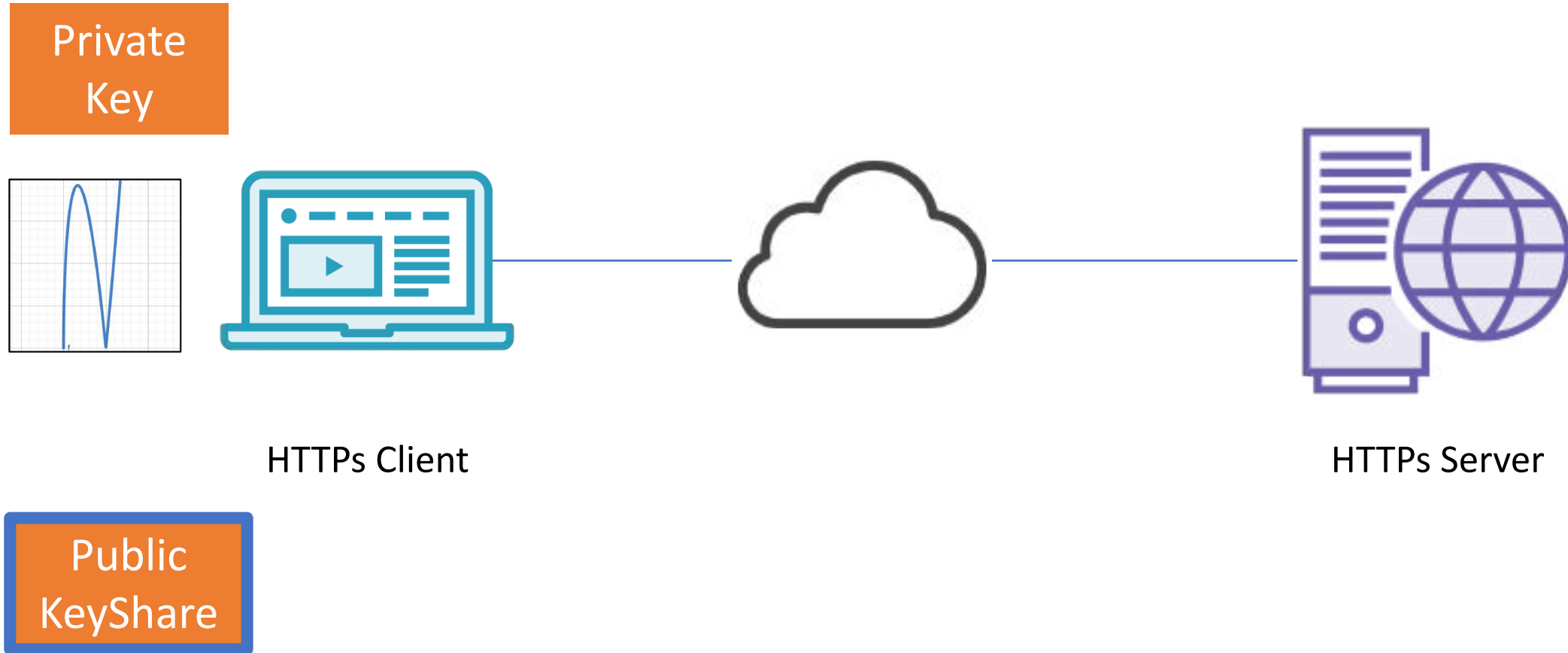
Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

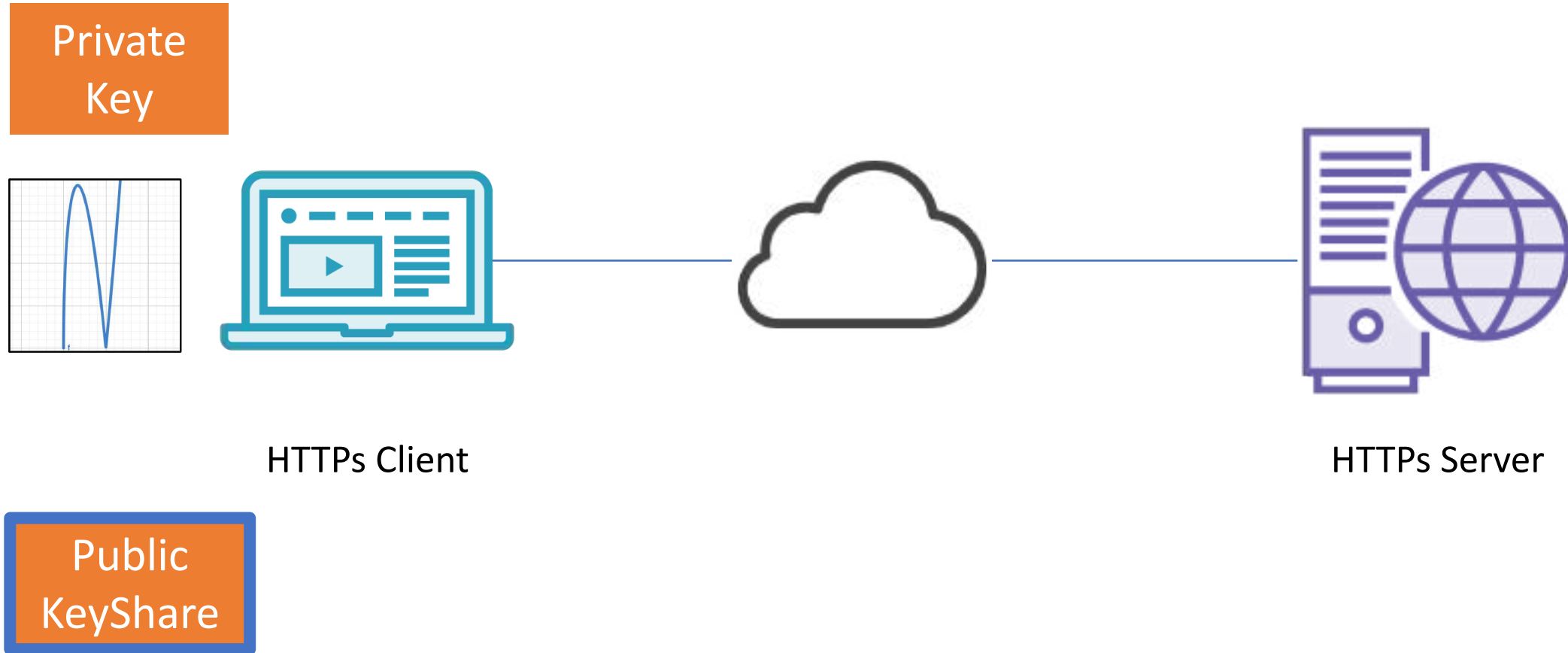
Public Key Share

500fb57e7b13fbaa8fa2630f79481db38c7189ef2ee10ab32797bcf9d8243753

# TLS 1.3 ECDHE Key Exchange



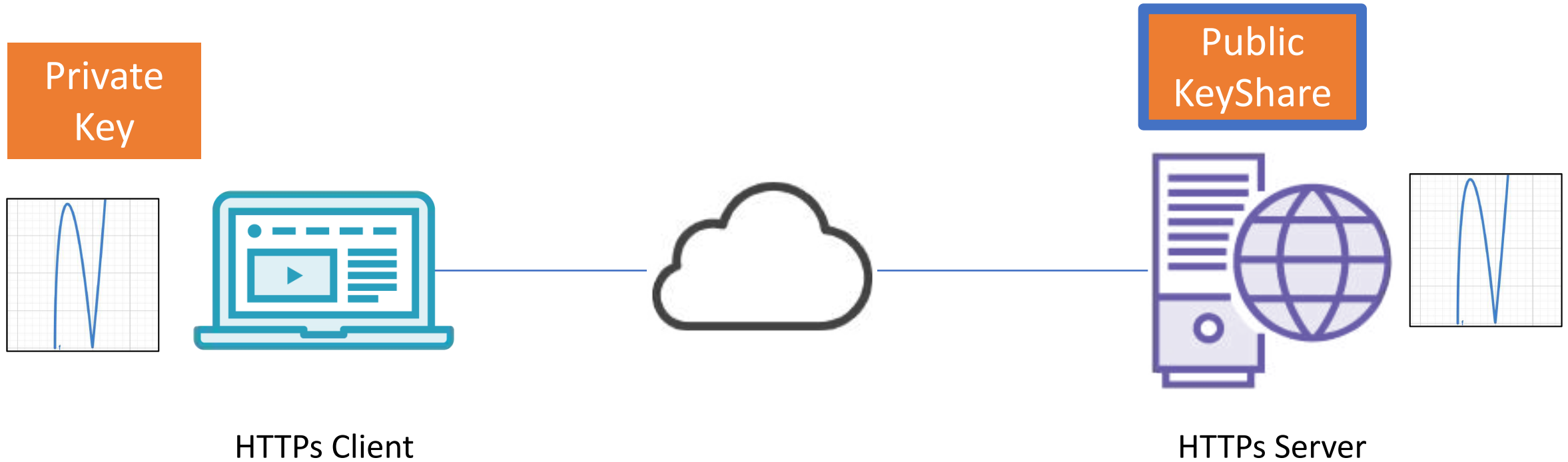
# TLS 1.3 ECDHE Key Exchange



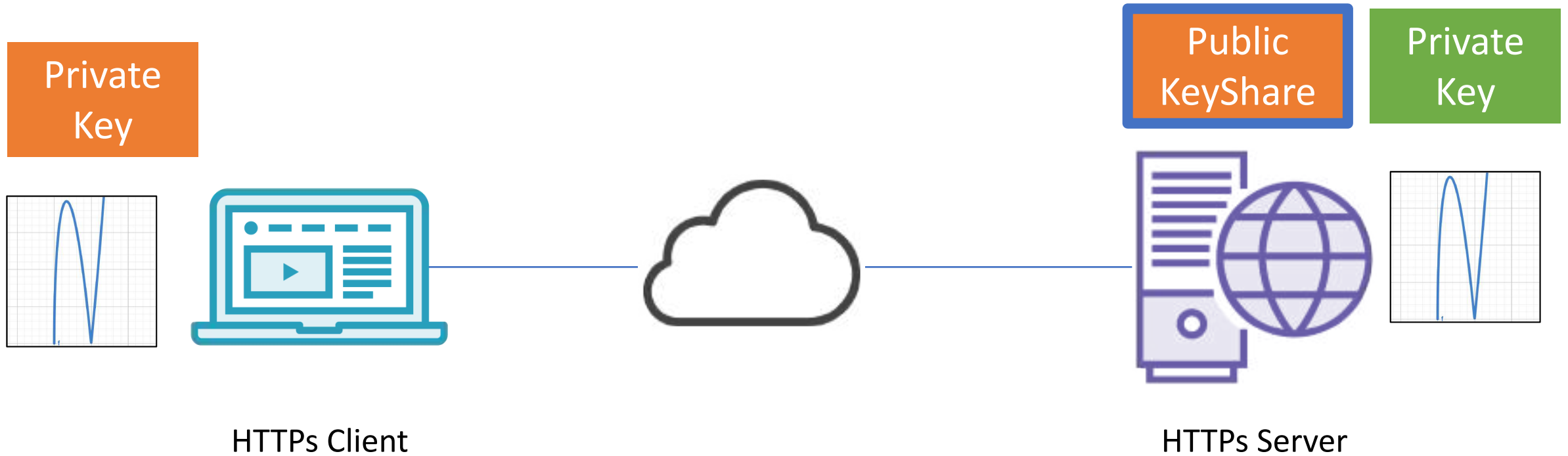
# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange

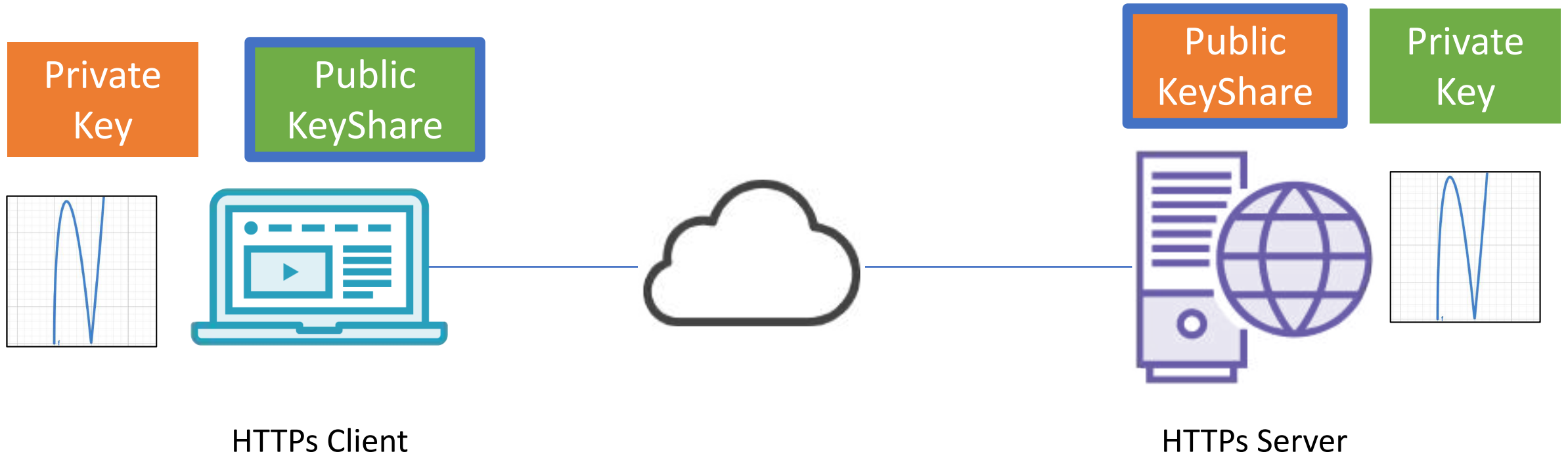




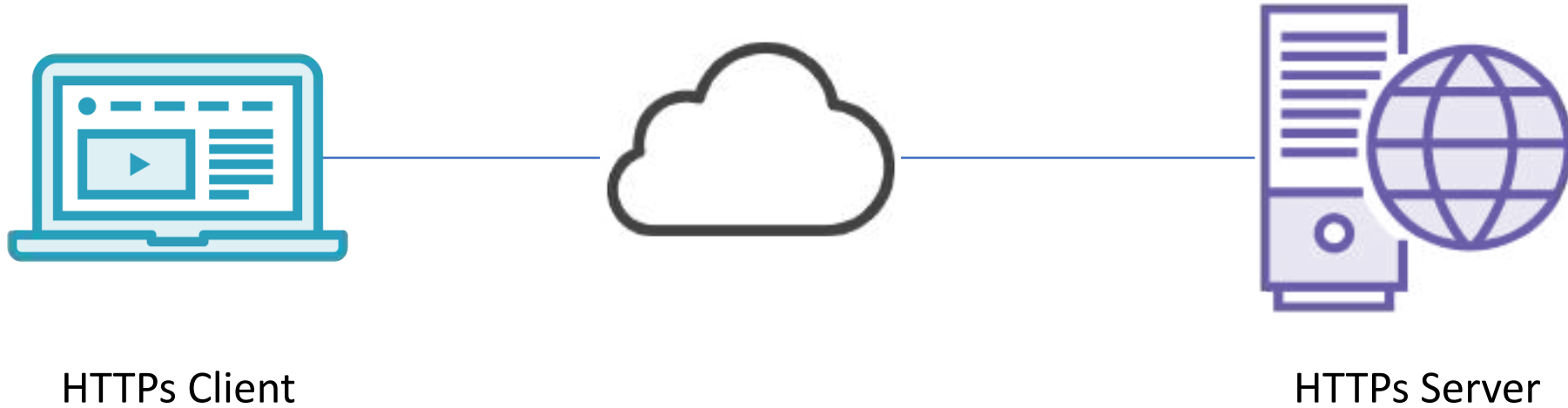
# TLS 1.3 ECDHE Key Exchange



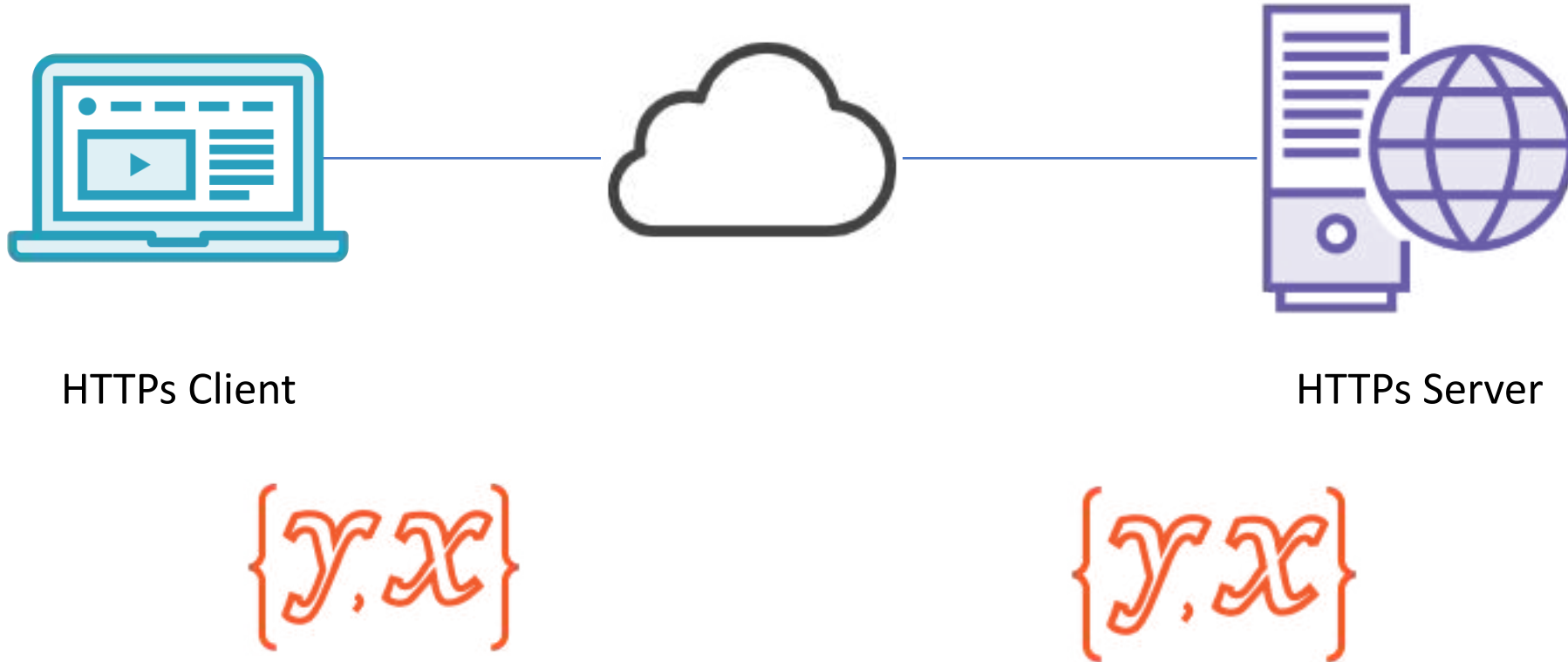
# TLS 1.3 ECDHE Key Exchange



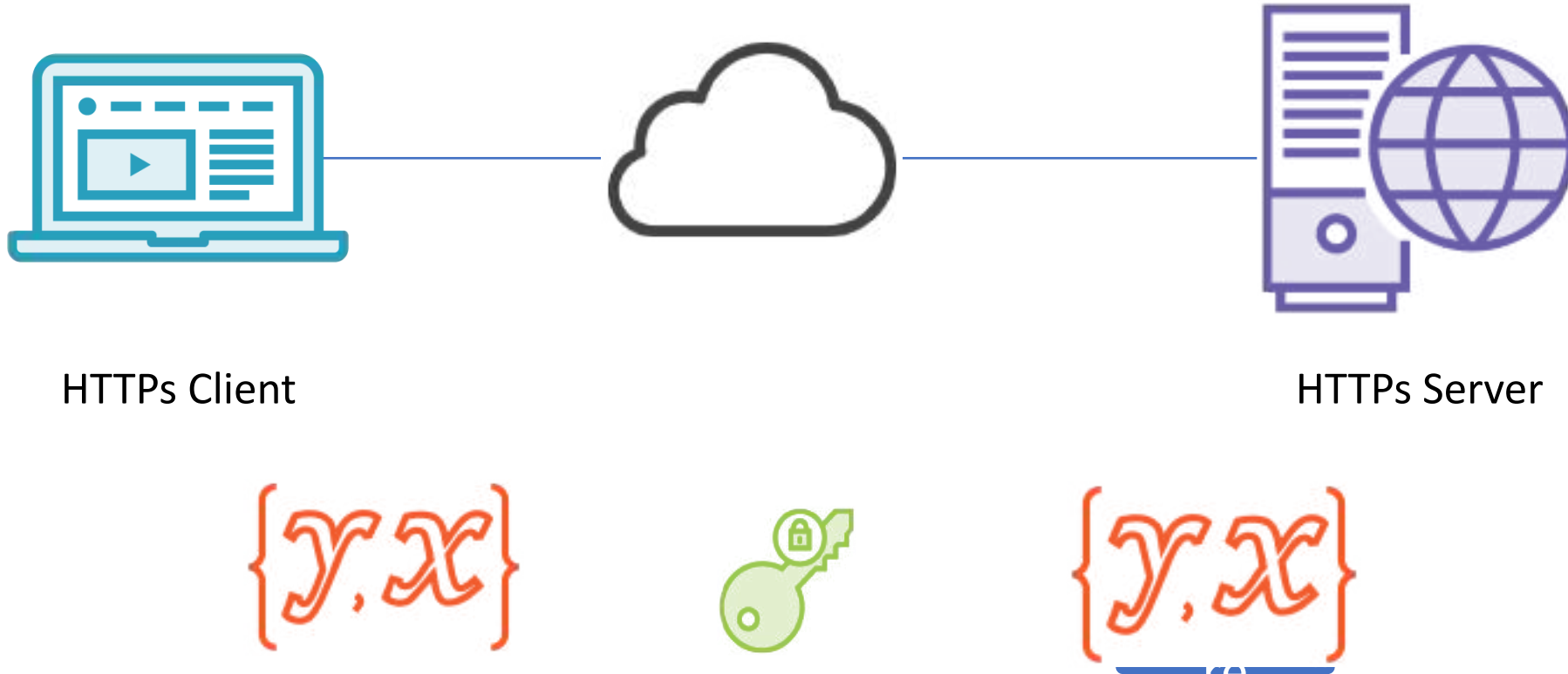
# TLS 1.3 ECDHE Key Exchange



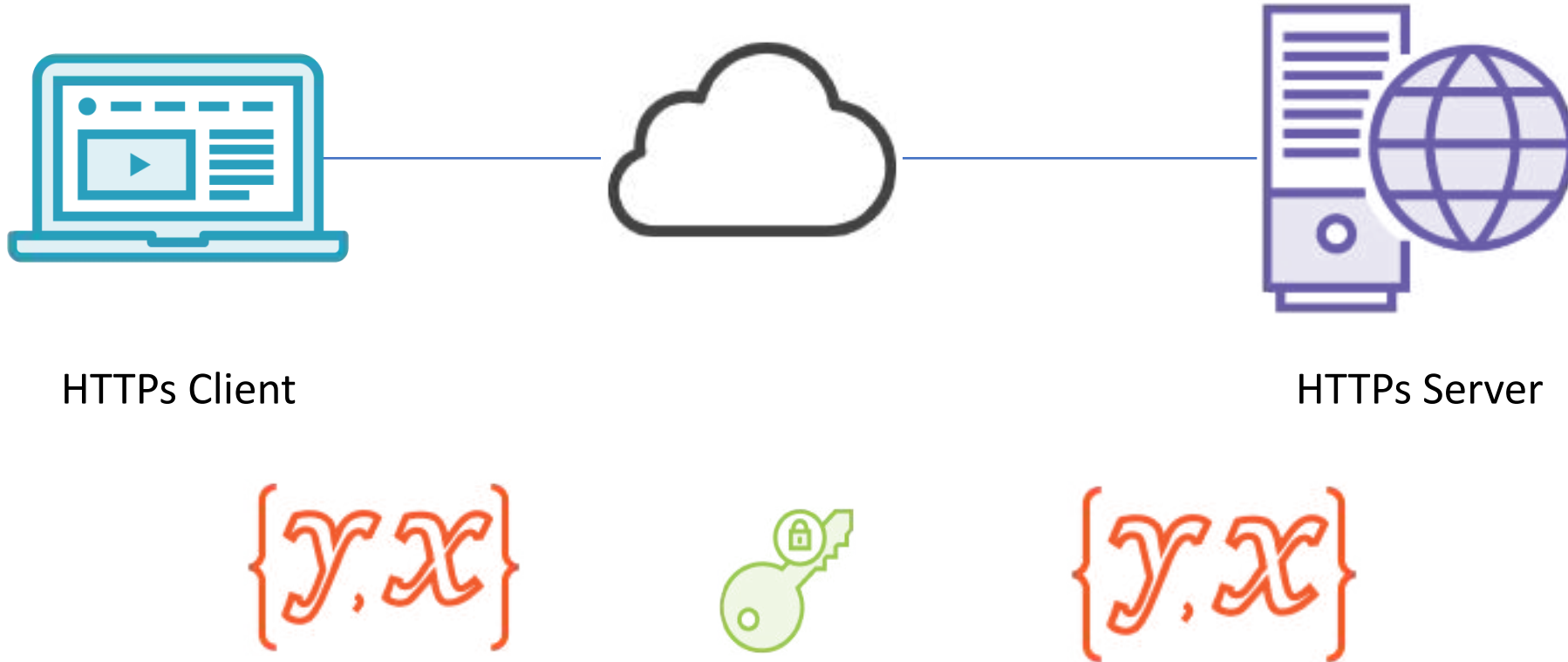
# TLS 1.3 ECDHE Key Exchange



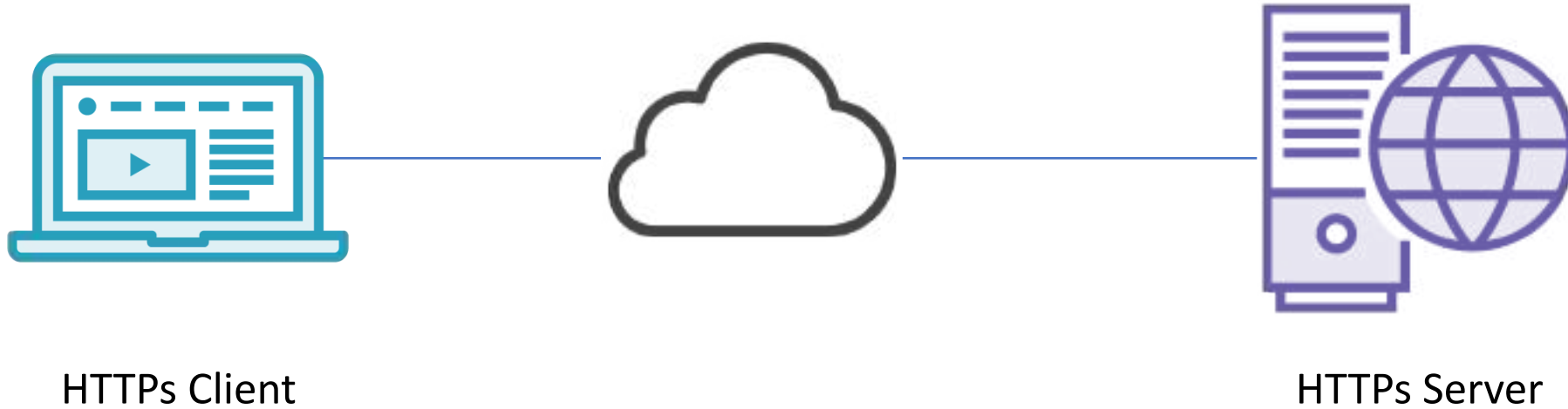
# TLS 1.3 ECDHE Key Exchange



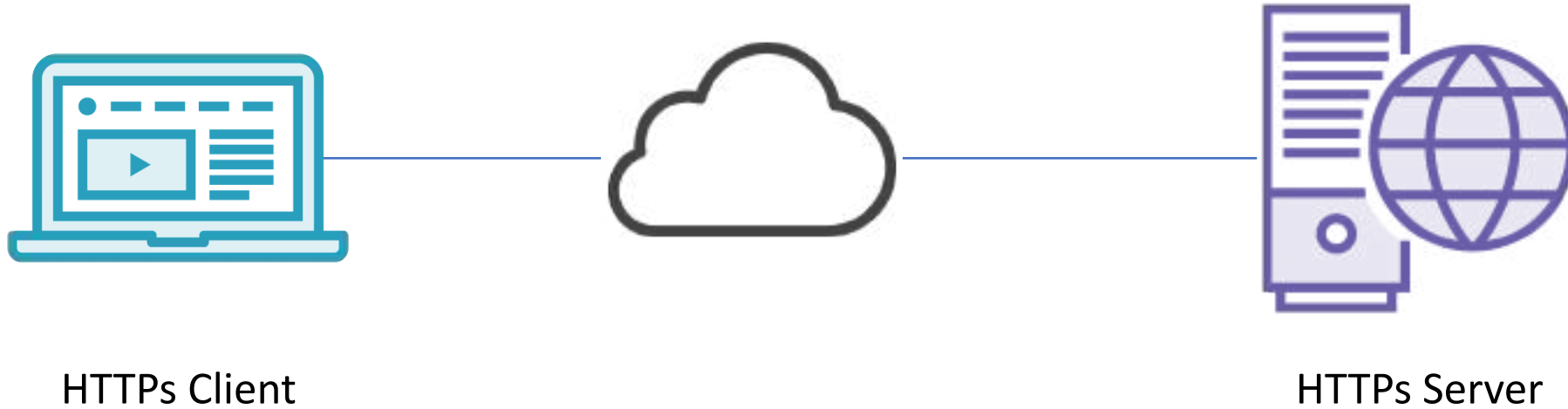
# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange

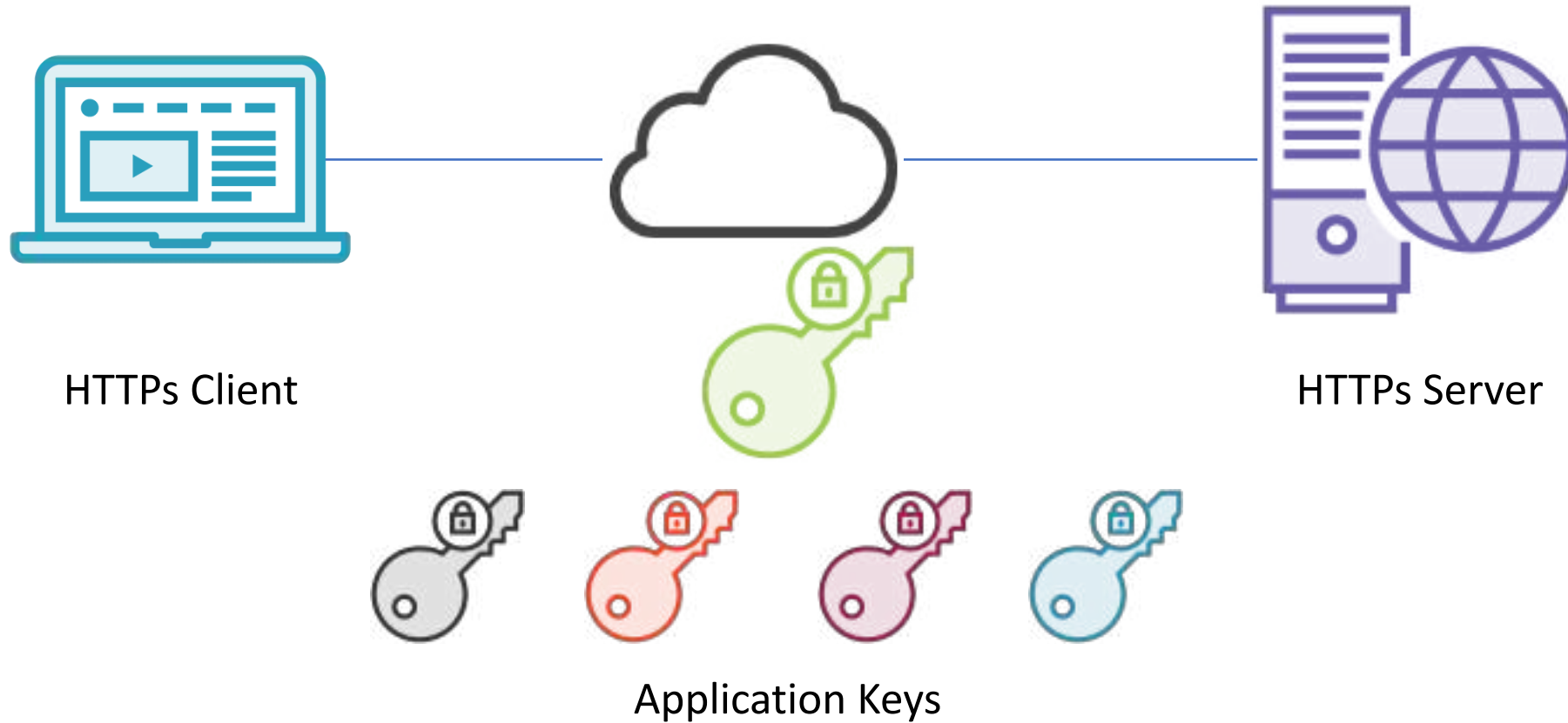


# TLS 1.3 ECDHE Key Exchange





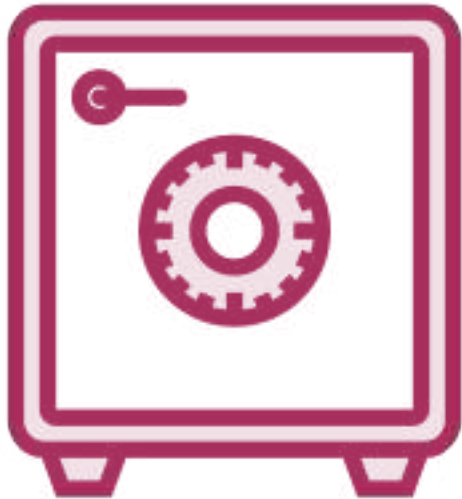
# TLS 1.3 ECDHE Key Exchange



# Elliptical Curve Diffie Hellman

# Data Encryption Protocols

## Ciphers



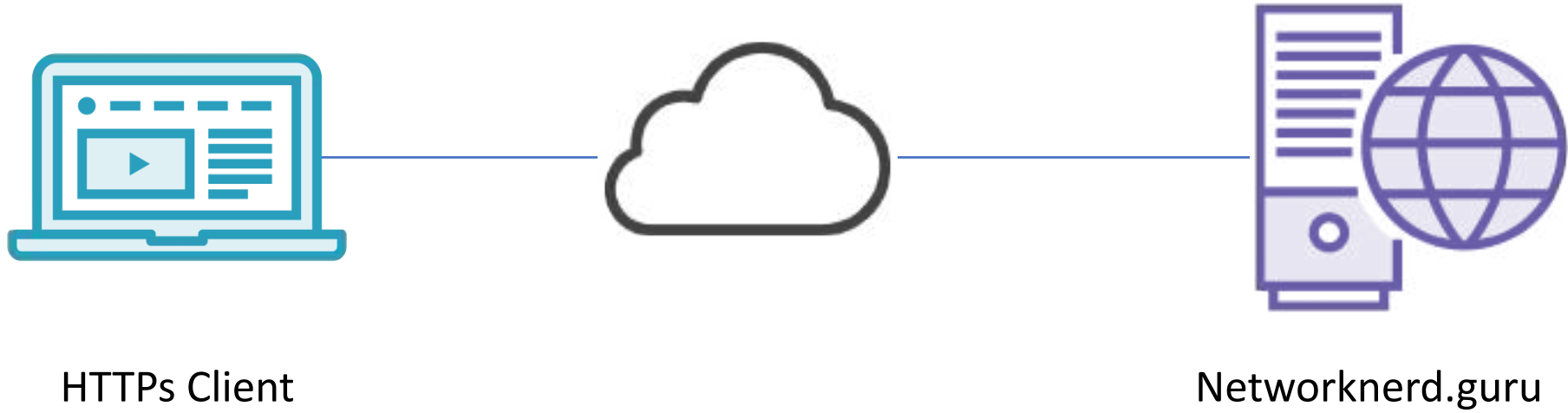
- 3DES (168 bit)
- AES (128 or 256 bits)
- ChaCha20

Key  
Exchange

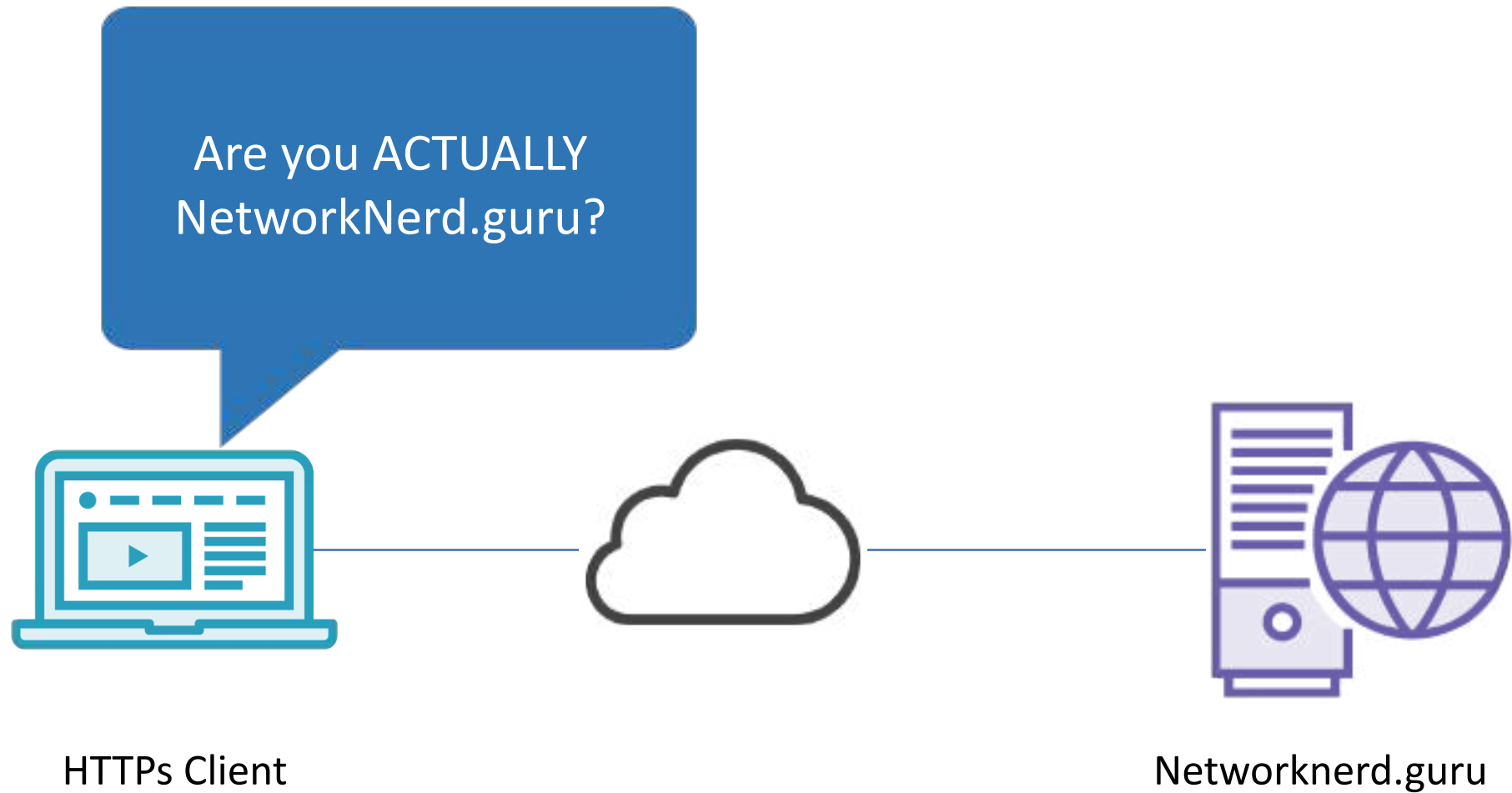
Data Encryption

Certificate

# Certificates

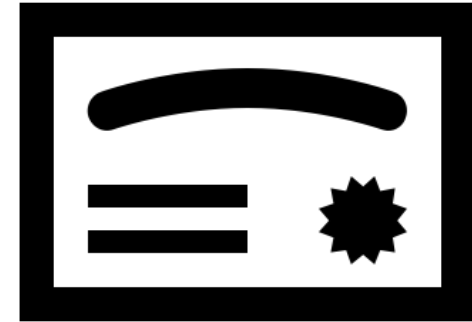


# Certificates



# Certificates

YES, OF COURSE  
I'm Networker.d.guru



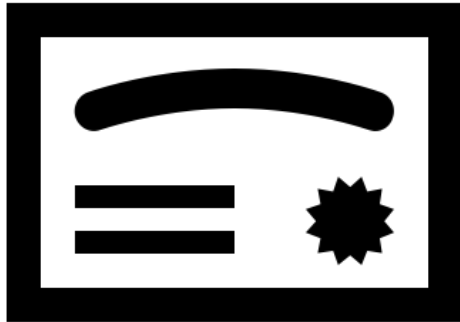
HTTPs Client



Networkner.d.guru

# Certificates

YES, OF COURSE  
I'm Networker.d.guru



HTTPs Client

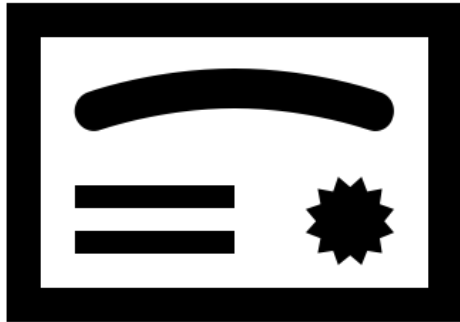


Networkner.d.guru



# Certificates

YES, OF COURSE  
I'm Networker.d.guru



HTTPs Client

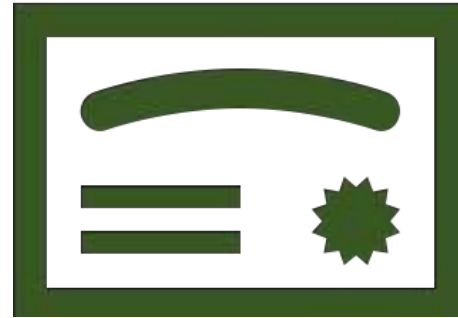


Networkner.d.guru

# Certificates

Certificate Authority (CA)

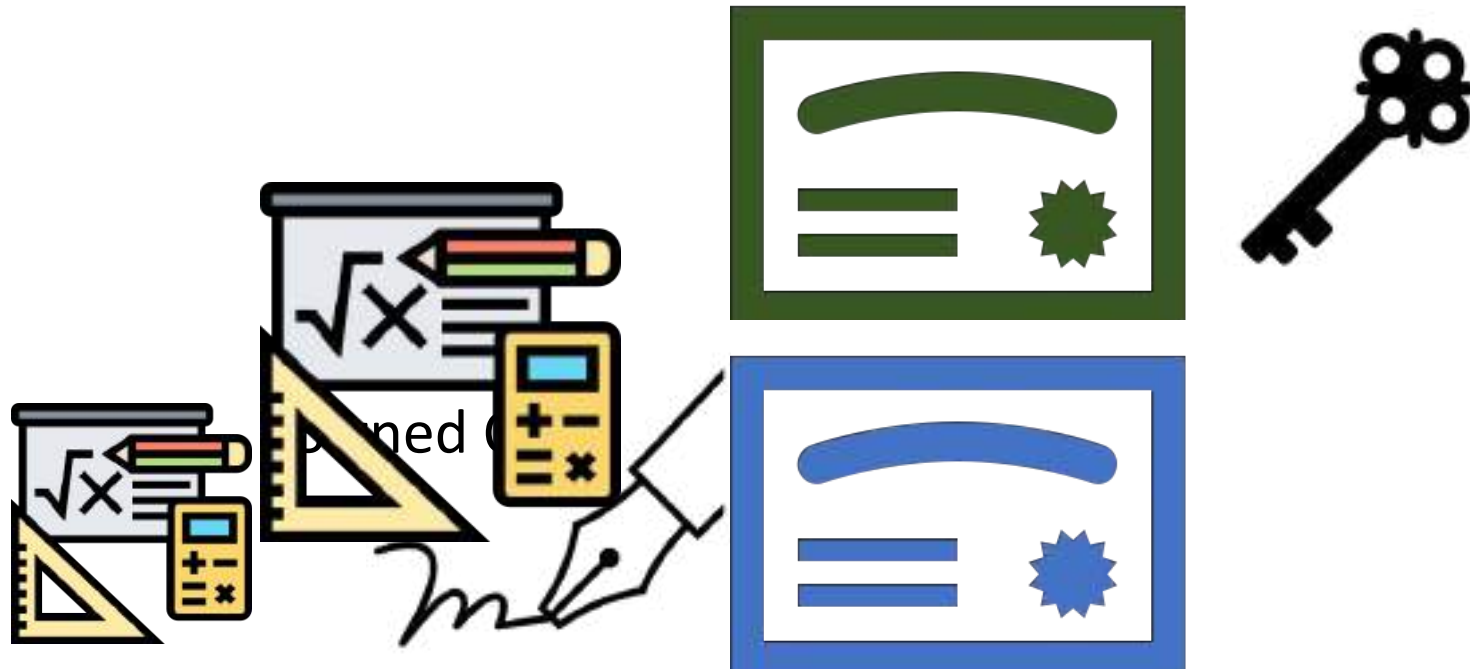
LetsEncrypt!



# Certificates

Certificate Authority (CA)

LetsEncrypt!

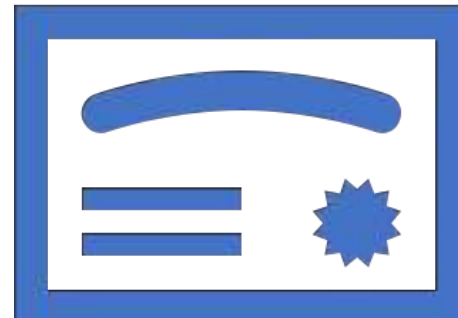
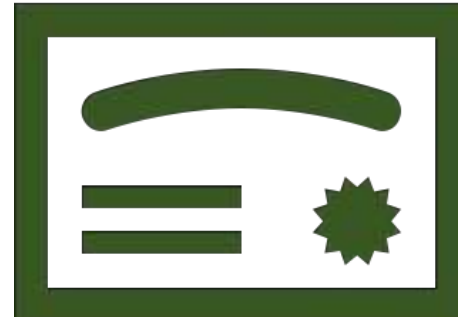


Intermediate Certificate

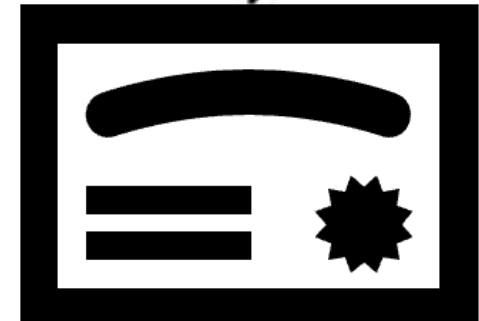
# Certificates

Certificate Authority (CA)

LetsEncrypt!



Intermediate Certificate

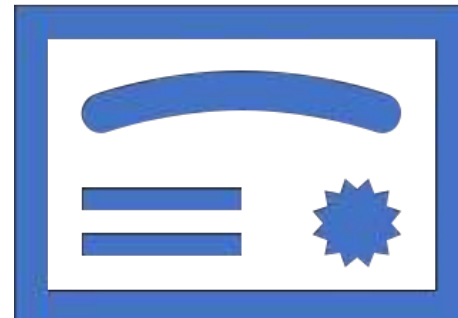
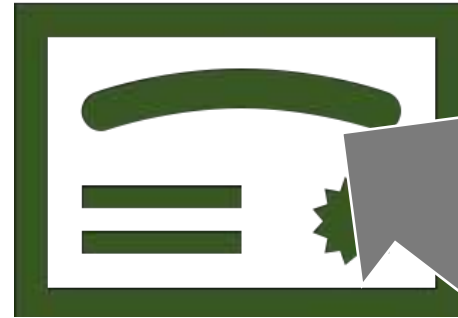


NetworkNerd.guru

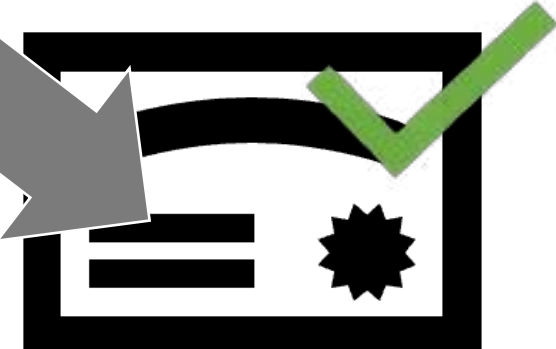
# Certificates

Certificate Authority (CA)

LetsEncrypt!



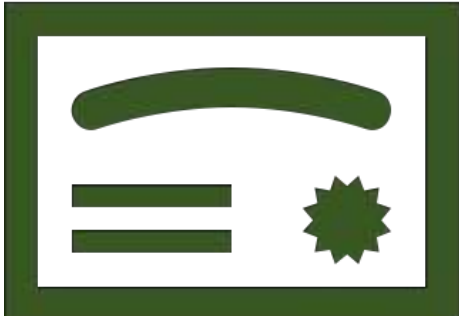
Intermediate Certificate



NetworkNerd.guru

# Certificates

Certificate Authority (CA)



Operating System  
Browser  
Certificate Store



HTTPs Client

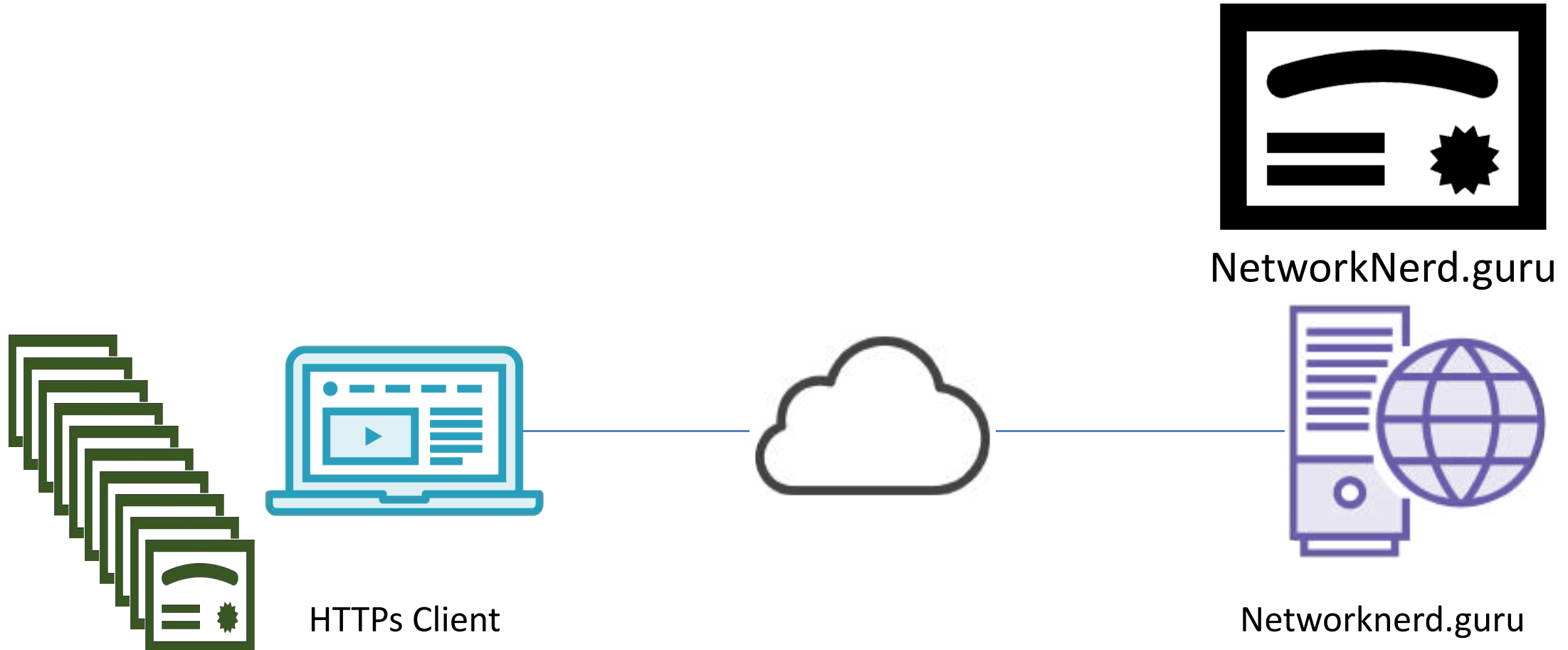


Networknerd.guru

# Certificates

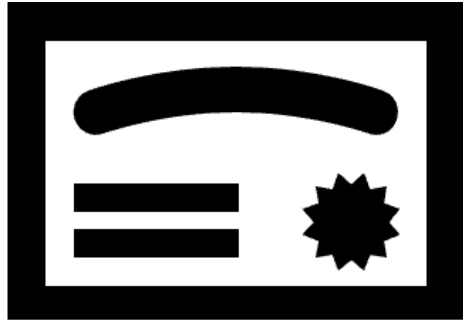


# Certificates





# Certificates



NetworkNerd.guru



HTTPs Client



Networknerd.guru

# The Design

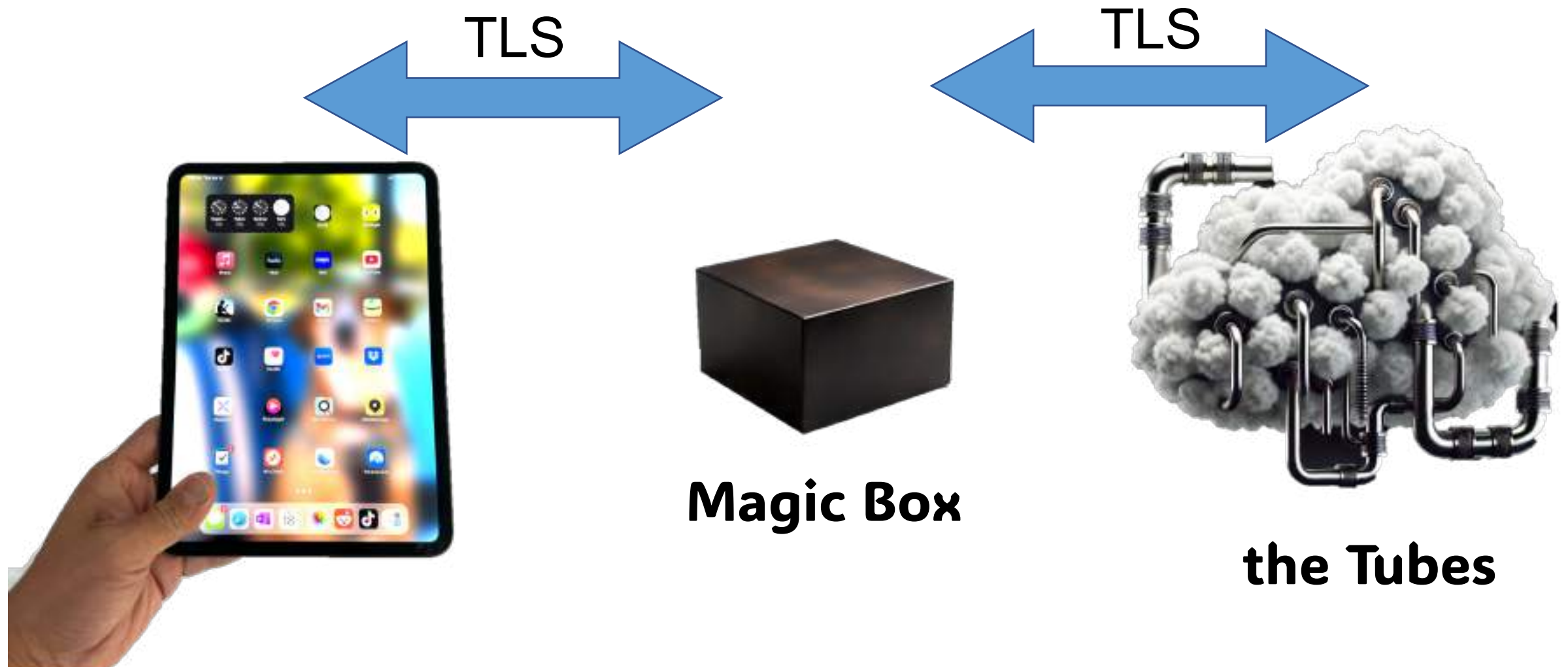


**Magic Box**

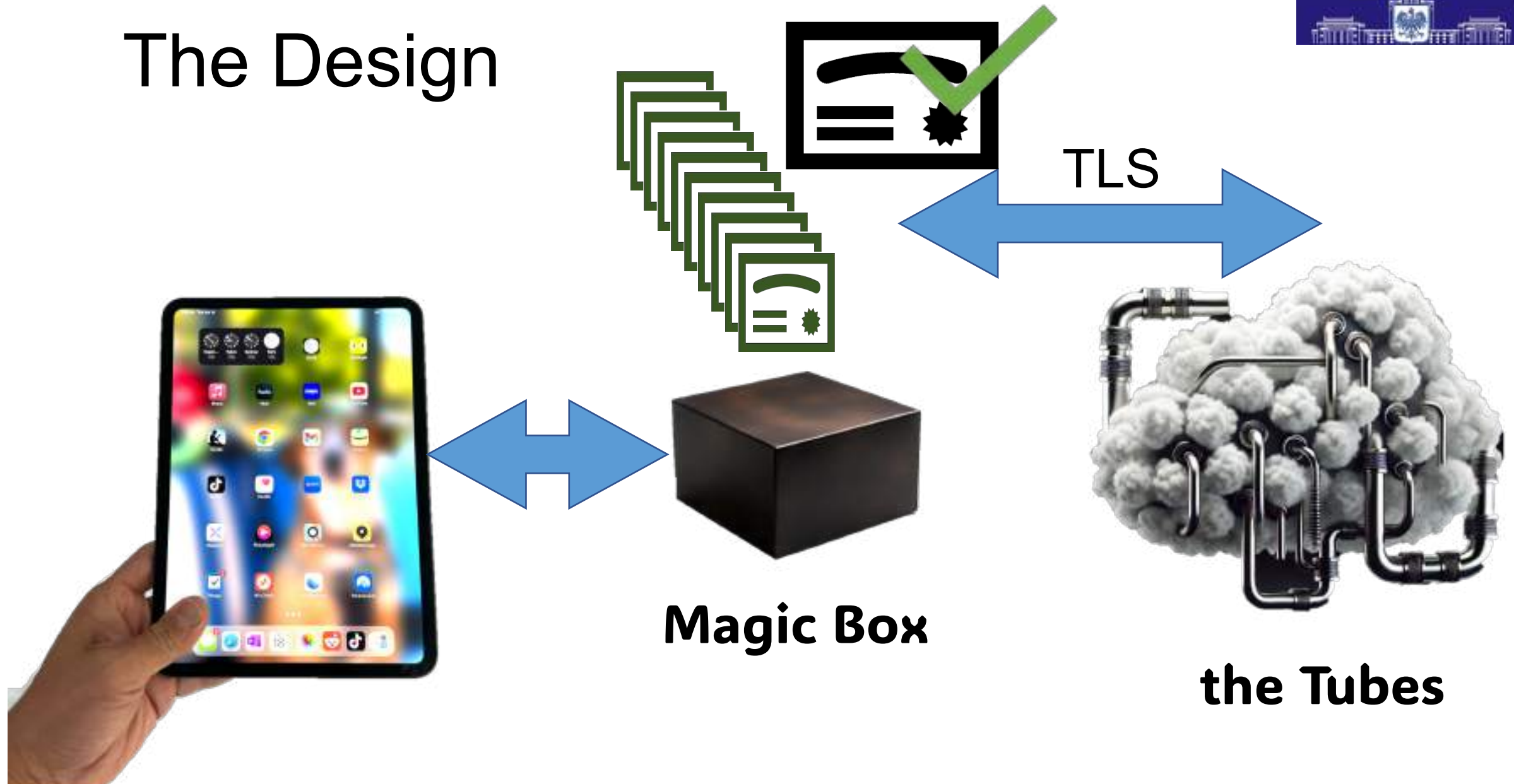


**the Tubes**

# The Design



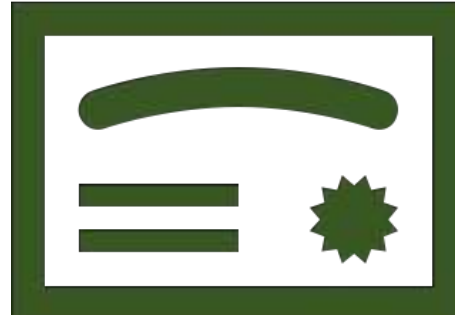
# The Design





# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**

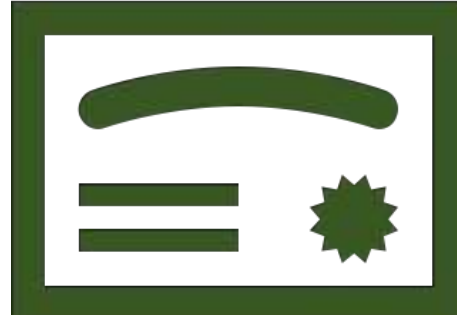


**the Tubes**



# The Design

Certificate Authority (CA)  
MITMproxy



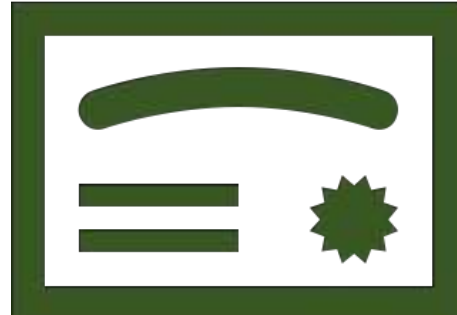
**Magic Box**



**the Tubes**

# The Design

Certificate Authority (CA)  
MITMproxy



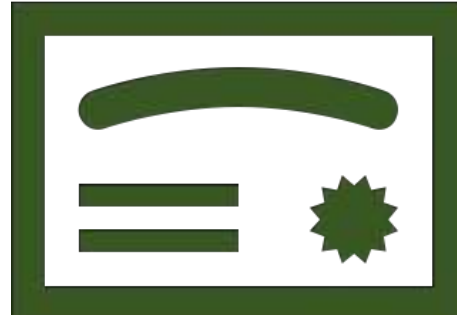
**Magic Box**



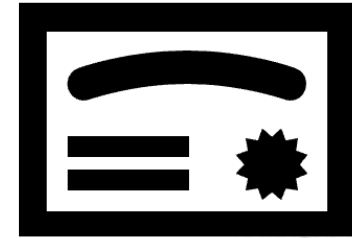
**the Tubes**

# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**



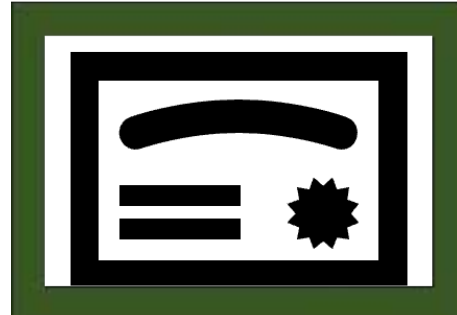
**the Tubes**



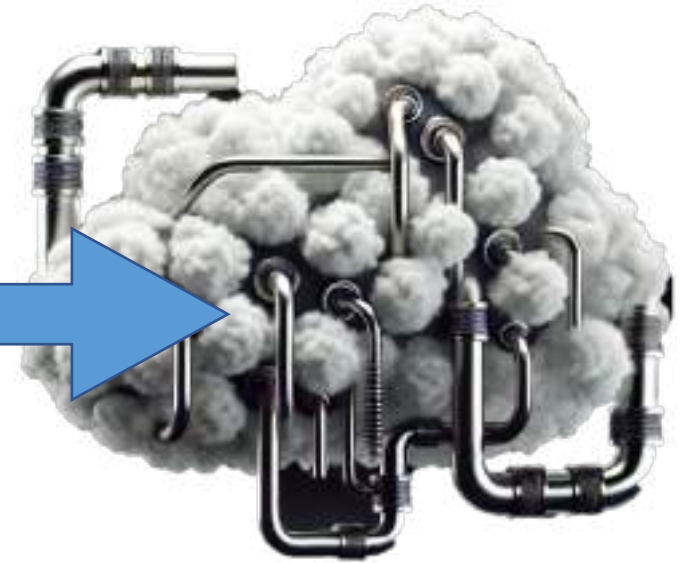


# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**

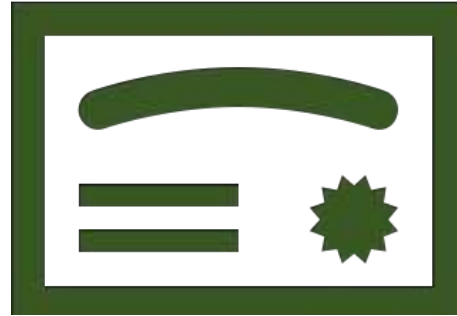


**the Tubes**

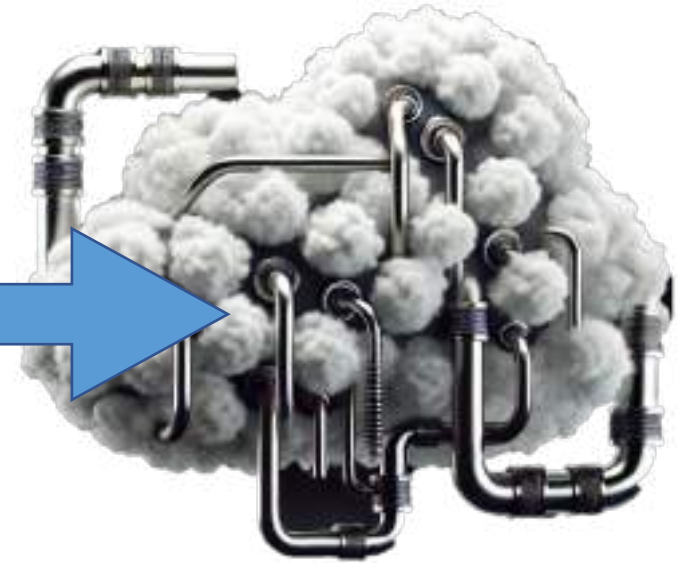


# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**



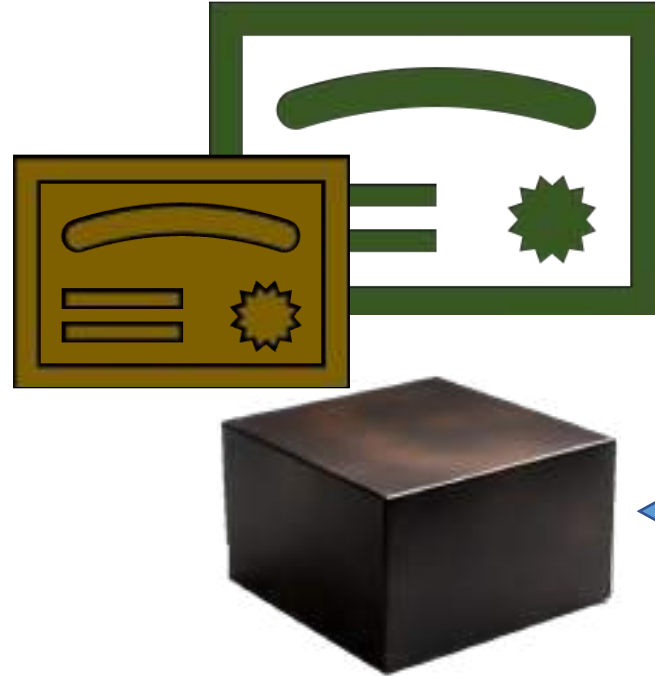
**the Tubes**



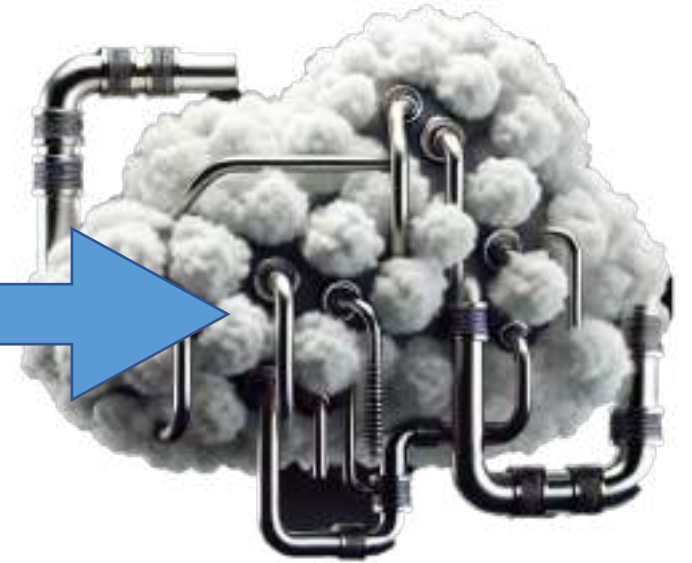
# The Design



Certificate Authority (CA)  
MITMproxy



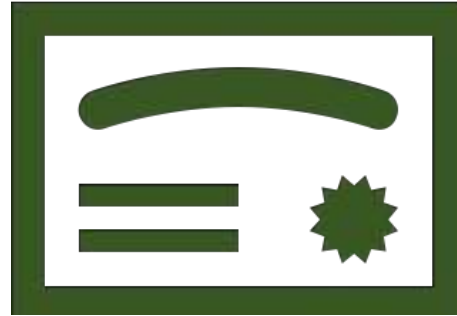
**Magic Box**



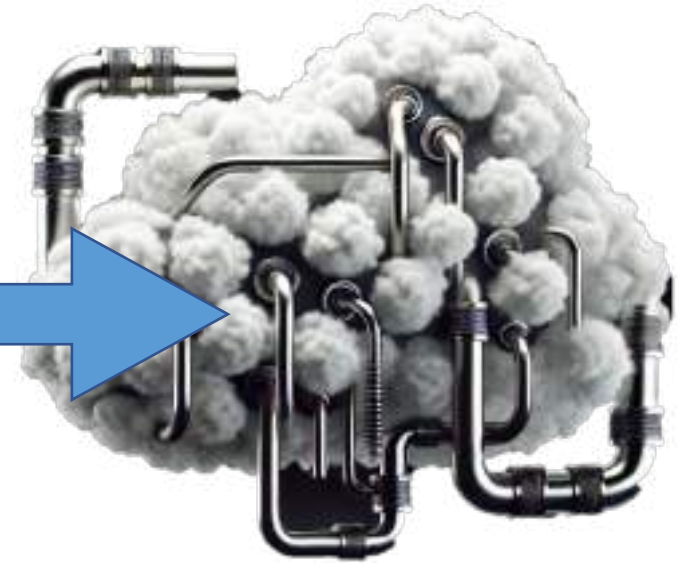
**the Tubes**

# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**



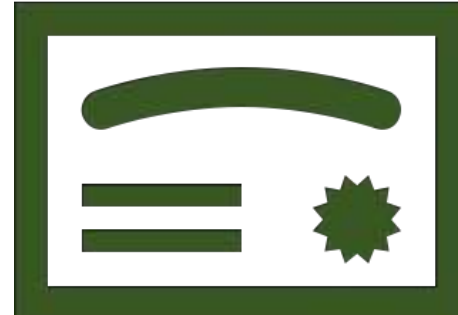
**the Tubes**



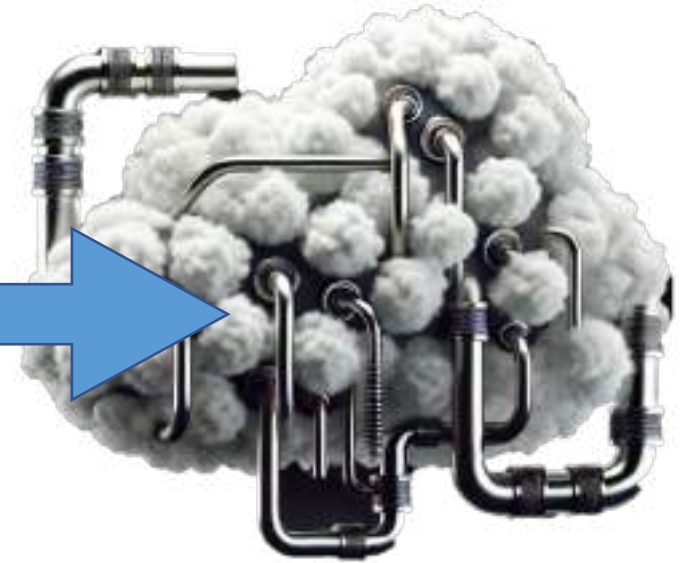


# The Design

Certificate Authority (CA)  
MITMproxy



**Magic Box**



**the Tubes**



# The Design



**Magic Box**



**the Tubes**

# The Design



**Magic Box**



2 Wireless Adapters

# The Design

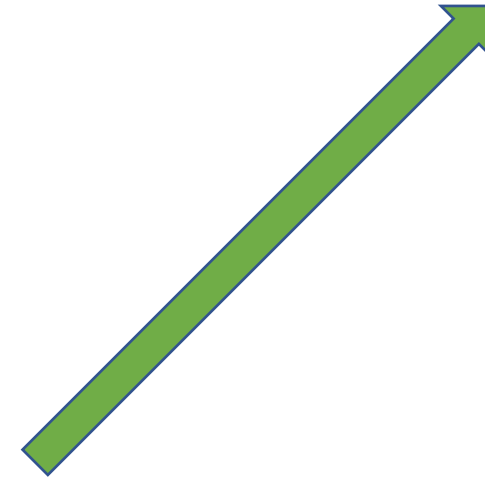


**Magic Box**



2 Wireless Adapters

Wireless NIC 1  
Connect to Local WiFi





# The Design

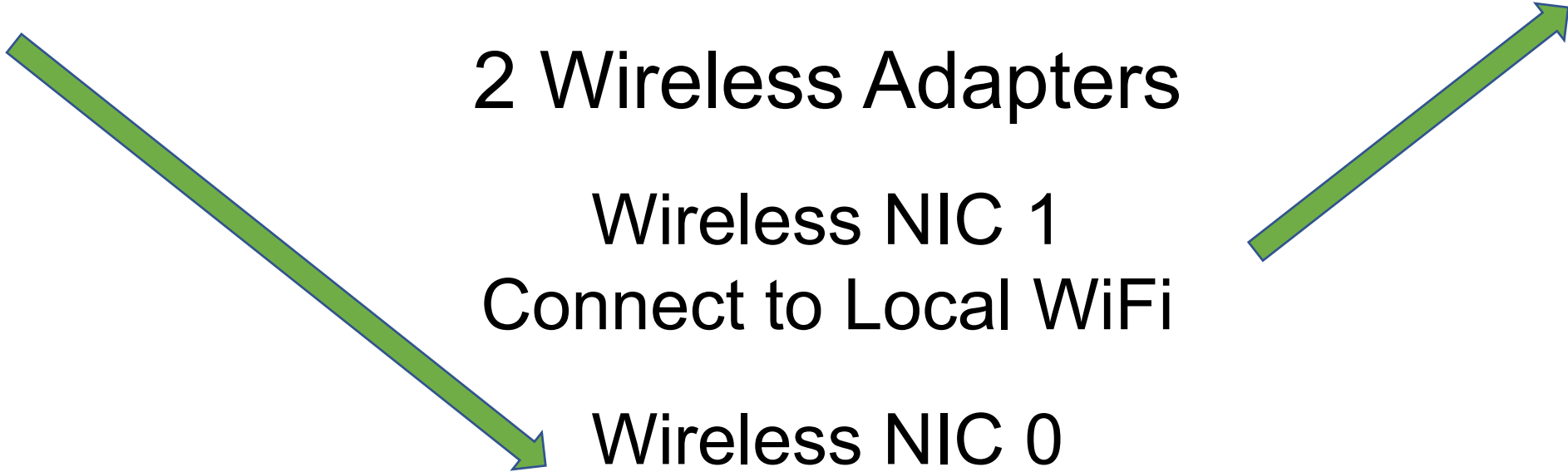


**Magic Box**

2 Wireless Adapters

Wireless NIC 1  
Connect to Local WiFi

Wireless NIC 0  
Access Point



# The Design



**Magic Box**

2 Wireless  
Adapters



Service to create  
Access Point  
HostAPD

# The Design



**Magic Box**



2 Wireless  
Adapters

HostAPD  
DNSmasq

# The Design



**Magic Box**



2 Wireless  
Adapters

HostAPD  
DNSmasq











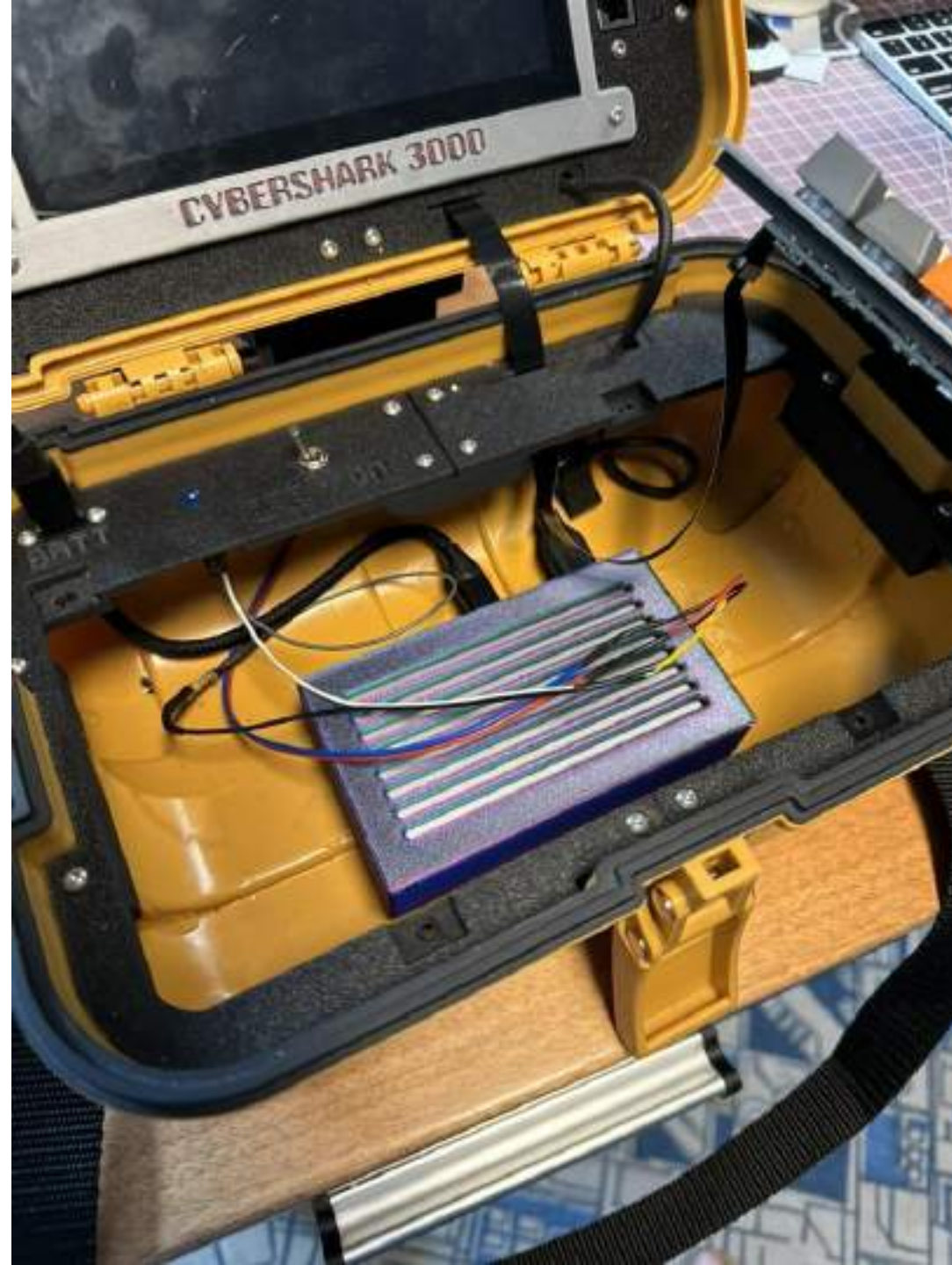












# Hardware Build

Raspberry Pi 5 – 8GB RAM

FREENOVE 7 Inch Touchscreen (800x480)

JJ50 KPrepublic keyboard PCB, key switch, key caps

MakerFocus Raspberry Pi 4 Battery Pack UPS,  
10000MAh

AT-B3 Surveying Transit Case

[https://www.ebay.com/sch/i.html?\\_from=R40&\\_trksid=p2334524.m570.l1313&\\_nkw=topcon+at-3b+case&\\_sacat=0&\\_odkw=topcon+at-3b+casae&\\_osacat=0](https://www.ebay.com/sch/i.html?_from=R40&_trksid=p2334524.m570.l1313&_nkw=topcon+at-3b+case&_sacat=0&_odkw=topcon+at-3b+casae&_osacat=0)

3D Model from Printables

<https://www.printables.com/model/425691-at-b3-cyberdeck>

# Lessons Learned

## The Good Stuff

- Stronger Linux Skills
- AI is a great tool for syntax and service dependency
- Improved understanding of TLS 1.2 /1.3
- Clearer understanding of Wireless chipsets on Linux
  - Realtek BAD
  - MediaTek Good

# Lessons Learned

## The Not So Good Stuff

- AI is a terrible tool for syntax and service dependency.
- Smartphone/Tablet apps are doing a great job of preventing this tool from working.
  - Certificate validation
  - Certificate pinning
- Raspberry Pi 5 is not powerful enough.