

# Bake Your Own Pi: the Cybershark 3000



**Ross Bagurdes**

IT Educator and Engineer  
Bagurdes Technology



# Ross Bagurdes

25+ Years Experience in IT network engineering and education

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

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

[ross@bagurdestechnology.com](mailto:ross@bagurdestechnology.com)

# The Idea



#sf24us

# The Idea



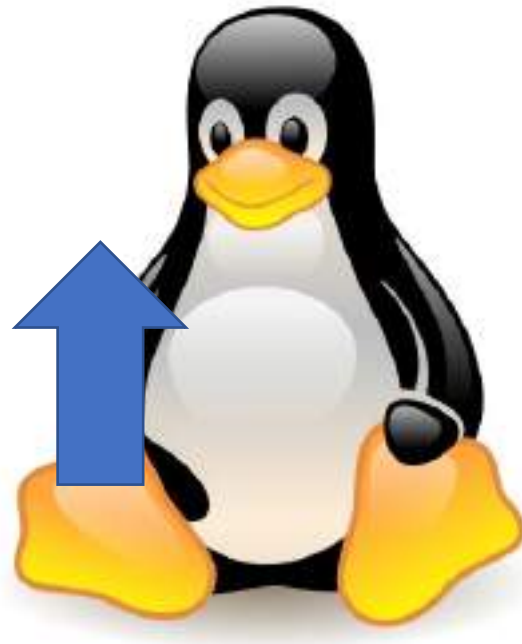
#sf24us





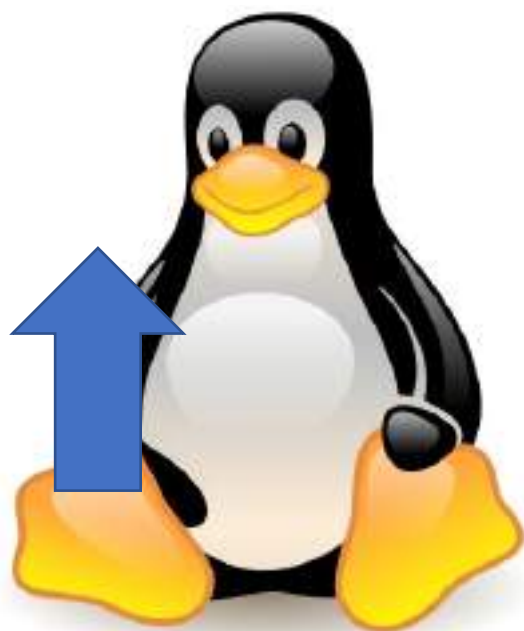


# Goals

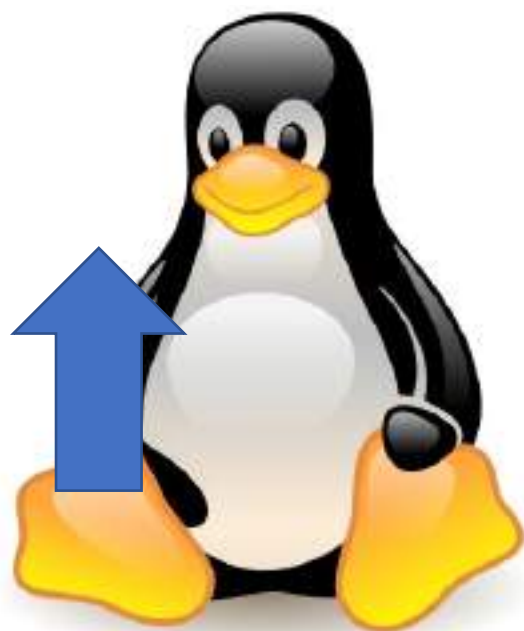




# Goals



# Goals





# The Design



**the Tubes**

# The Design



**Magic Box**



**the Tubes**

# The Design



**Magic Box**



**the Tubes**

# Data Encryption Basics





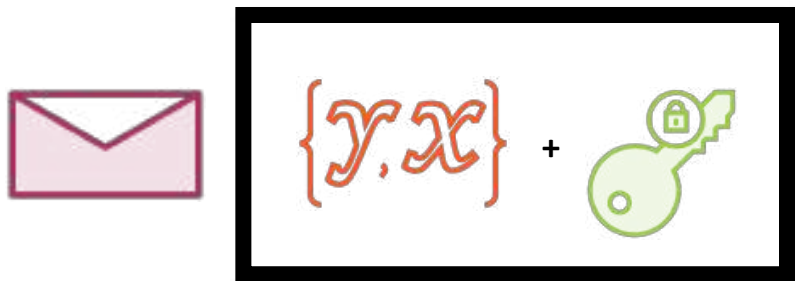
# Data Encryption Basics



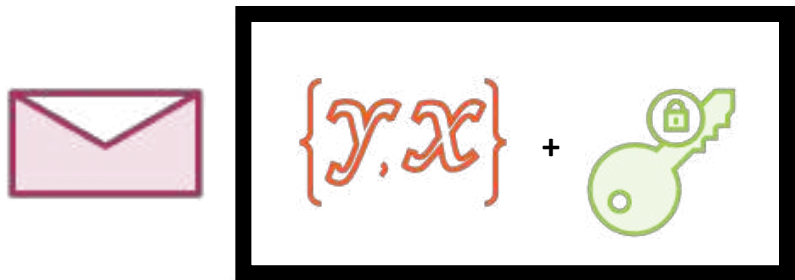
# Data Encryption Basics



# 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



HTTPs Client



HTTPs Server

# Data Encryption Basics



HTTPs Client



HTTPs Server





# Data Encryption Basics



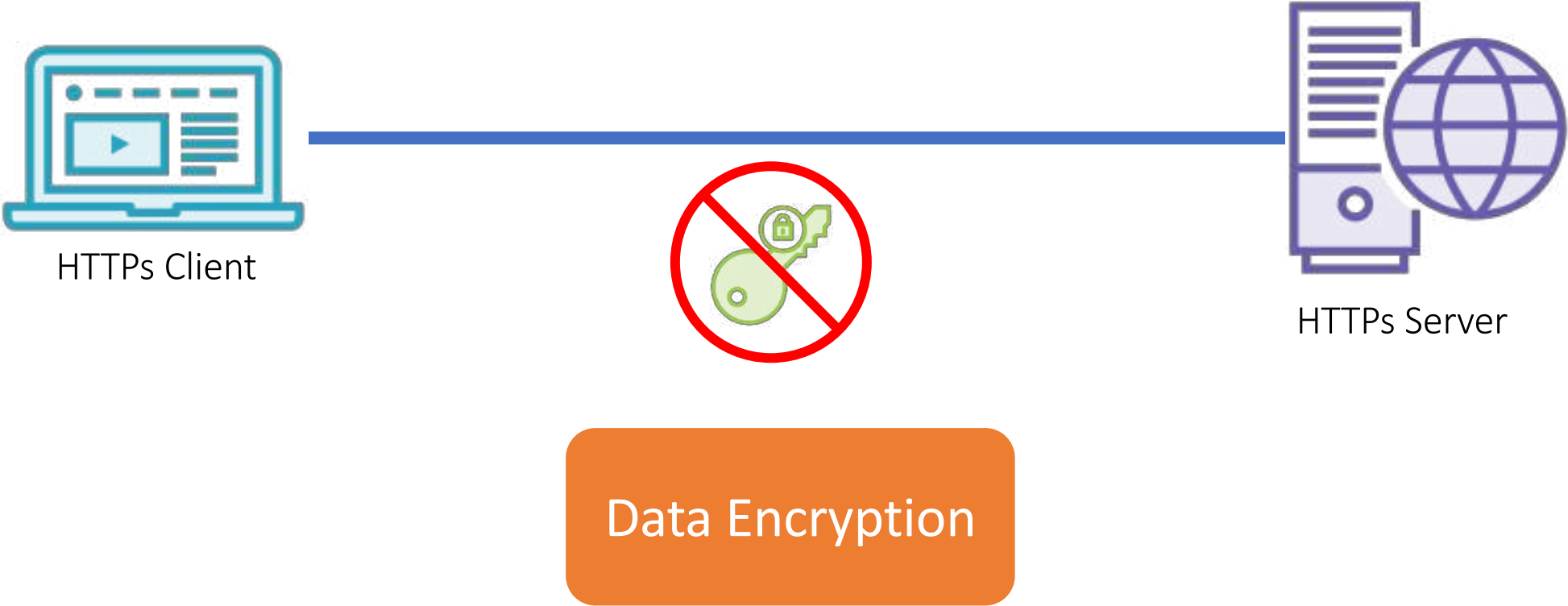
# Data Encryption Basics



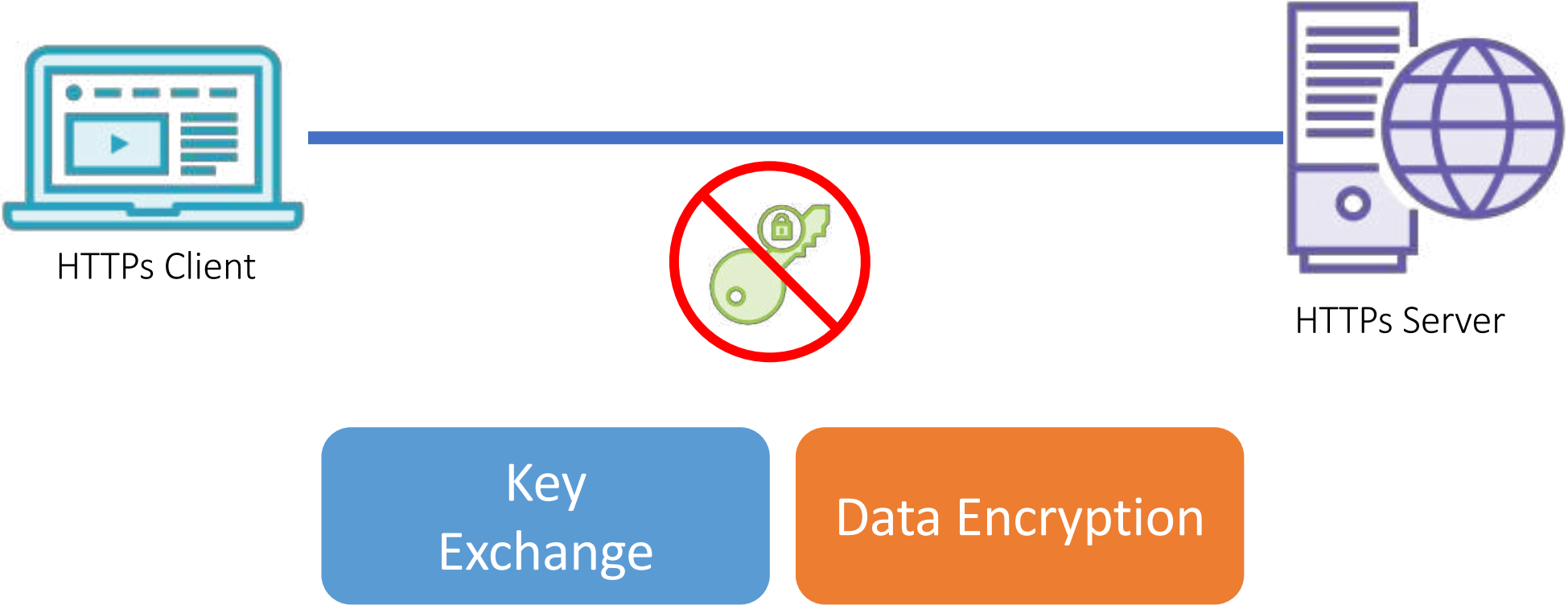
# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



# Exchanging the Secret Key



HTTPs Client



HTTPs Server





# Exchanging the Secret Key

SharkFest'24 US  
June 15-20 - Fairfax, VA

#sf24us



HTTPs Client



HTTPs Server



Rivest Shamir Adleman  
(RSA) 1977

# Exchanging the Secret Key



HTTPs Client



HTTPs Server



#sf24us



Rivest Shamir Adleman  
(RSA) 1977

Diffie-Hellman (and Merkle)  
(DH) 1976

# Exchanging the Secret Key

SharkFest'24 US  
June 15-20 - Fairfax, VA

#sf24us



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

Diffie-Hellman (and Merkle)  
(DH) 1976



HTTPs Client



HTTPs Server



SharkFest'24 US  
June 15-20 - Fairfax, VA

#sf24us

# Exchanging the Secret Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976



HTTPs Server

$p = 149$   
 $g = 17$

A blue outline icon of a ribbon seal with a scalloped edge, attached to the bottom right corner of the box.

# Exchanging the Secret Key




HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976



HTTPs Server

$p = 149$   
 $g = 17$





# Exchanging the Secret Key



HTTPs Client

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

# Exchanging the Secret Key



HTTPs Client

$a = 8$

Private Key

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

# Exchanging the Secret Key



HTTPs Client

$a = 8$

Private Key

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key



HTTPs Server

$b = 6$

Private Key

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

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

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

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

#sf24us

US

June 15-20 - Fairfax, VA

$a = 8$

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

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

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

US

June 15-20 - Fairfax, VA

#sf24us

$a = 8$

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

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

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



a = 8

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

p = 149  
g = 17

Public Key

b = 6

Private Key

#sf24us



HTTPs Server

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

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

a = 8

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

p = 149  
g = 17

Public Key



HTTPs Server

b = 6

Private Key

#sf24us

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

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



# Quick Math Lesson

95 divided by 8

95 divided by 8

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

95 divided by 8

$$8 \overline{) 95}$$

$$8 \overline{) 95}$$

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



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

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

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

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

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

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

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

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



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

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

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



#sf24us

11 r 7



#sf24us

r 7

95 mod 8

Modulus 7

a = 8

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

p = 149  
g = 17

Public Key



HTTPs Server

b = 6

Private Key

#sf24us

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

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

a = 8

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976

p = 149  
g = 17

Public Key

b = 6

Private Key

#sf24us



HTTPs Server

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

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

5 = Key Share(a)



# 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

$b = 6$

Private Key



HTTPs Server

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

US

June 15-20 - Fairfax, VA

#sf24us

# 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

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

$b = 6$

Private Key



HTTPs Server

#sf24us

US

June 15-20 - Fairfax, VA

# 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

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

$b = 6$

Private Key



HTTPs Server

#sf24us

US

June 15-20 - Fairfax, VA

# 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

$b = 6$

Private Key



HTTPs Server

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

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

US

June 15-20 - Fairfax, VA

#sf24us

# 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

$b = 6$

Private Key



HTTPs Server

16

Key Share(b)

#sf24us

US

June 15-20 - Fairfax, VA

# 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

$b = 6$

Private Key



HTTPs Server

16

Key Share(b)

#sf24us

US

June 15-20 - Fairfax, VA

# 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

$b = 6$

Private Key



HTTPs Server

5

Key Share(a)

#sf24us

US

June 15-20 - Fairfax, VA

# Exchanging the Secret Key

$a = 8$

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

$b = 6$

Private Key



HTTPs Server

5

Key Share(a)

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

US

June 15-20 - Fairfax, VA

#sf24us



# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

16

Key Share(b)

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

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

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

5

Key Share(a)

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

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

US

June 15-20 - Fairfax, VA

#sf24us

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

16

Key Share(b)

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

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

129

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

5

Key Share(a)

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

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

US

June 15-20 - Fairfax, VA

#sf24us

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

16

Key Share(b)

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

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

129

Diffie-Hellman (and Merkle)  
(DH) 1976

$p = 149$   
 $g = 17$

Public Key

$b = 6$

Private Key



HTTPs Server

5

Key Share(a)

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

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

129

US

June 15-20 - Fairfax, VA

#sf24us

# Exchanging the Secret Key

$a = 8$

Private Key



HTTPs Client

$b = 6$

Private Key



HTTPs Server

Diffie-Hellman (and Merkle)  
(DH) 1976

16

Key  
Share(b)

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

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

129



5

Key  
Share(a)

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

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

129



$a = 8$

Private Key



HTTPs Client

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976



$b = 6$

Private Key



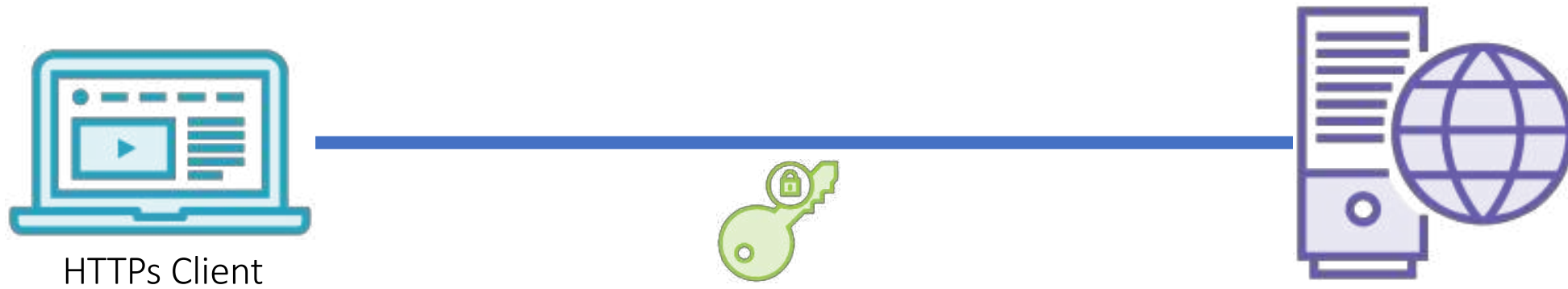
#sf24us

US

June 15-20 - Fairfax, VA

# Exchanging the Secret Key

Diffie-Hellman (and Merkle)  
(DH) 1976



HTTPs Client



# 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

RSA

Diffie Hellman

Elliptical Curve

Diffie Hellman

Key  
Exchange

TLS v1.3

# TLS Encryption

TLS v1.2

~~RSA~~

Diffie Hellman

Elliptical Curve  
Diffie Hellman

Key  
Exchange

TLS v1.3

# TLS Encryption

TLS v1.2

Key  
Exchange

TLS v1.3

~~RSA~~

~~Diffie Hellman~~

Elliptical Curve  
Diffie Hellman

# TLS Encryption

Key Exchange

TLS v1.2

~~RSA~~

~~Diffie Hellman~~

Elliptical Curve  
Diffie Hellman

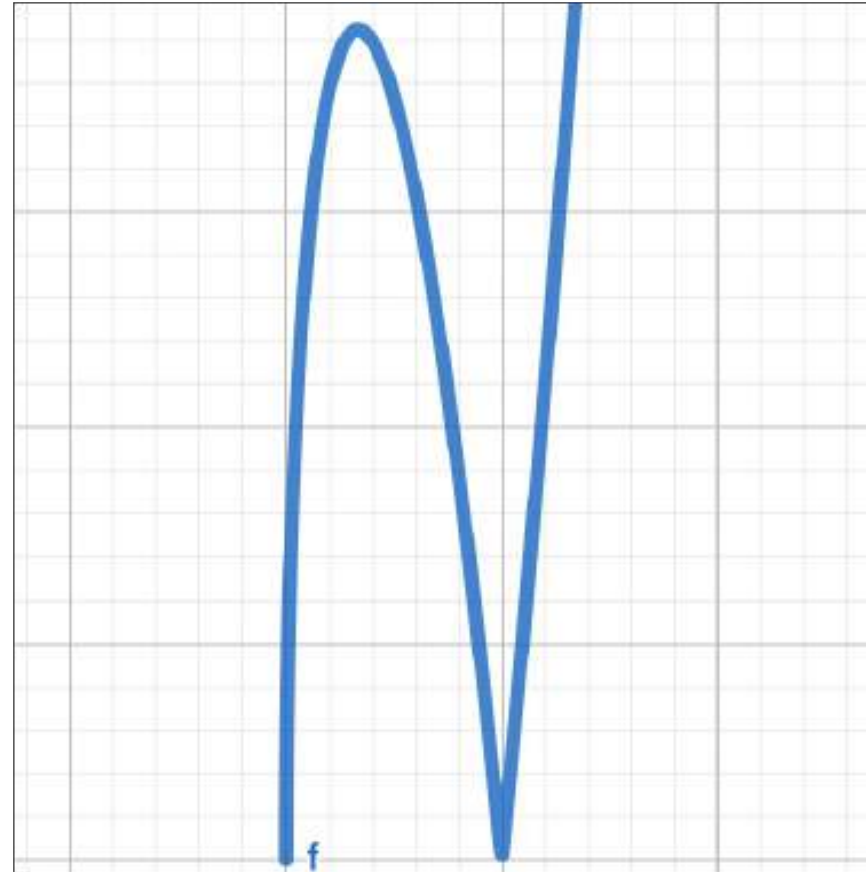
TLS v1.3

Elliptical Curve  
Diffie Hellman



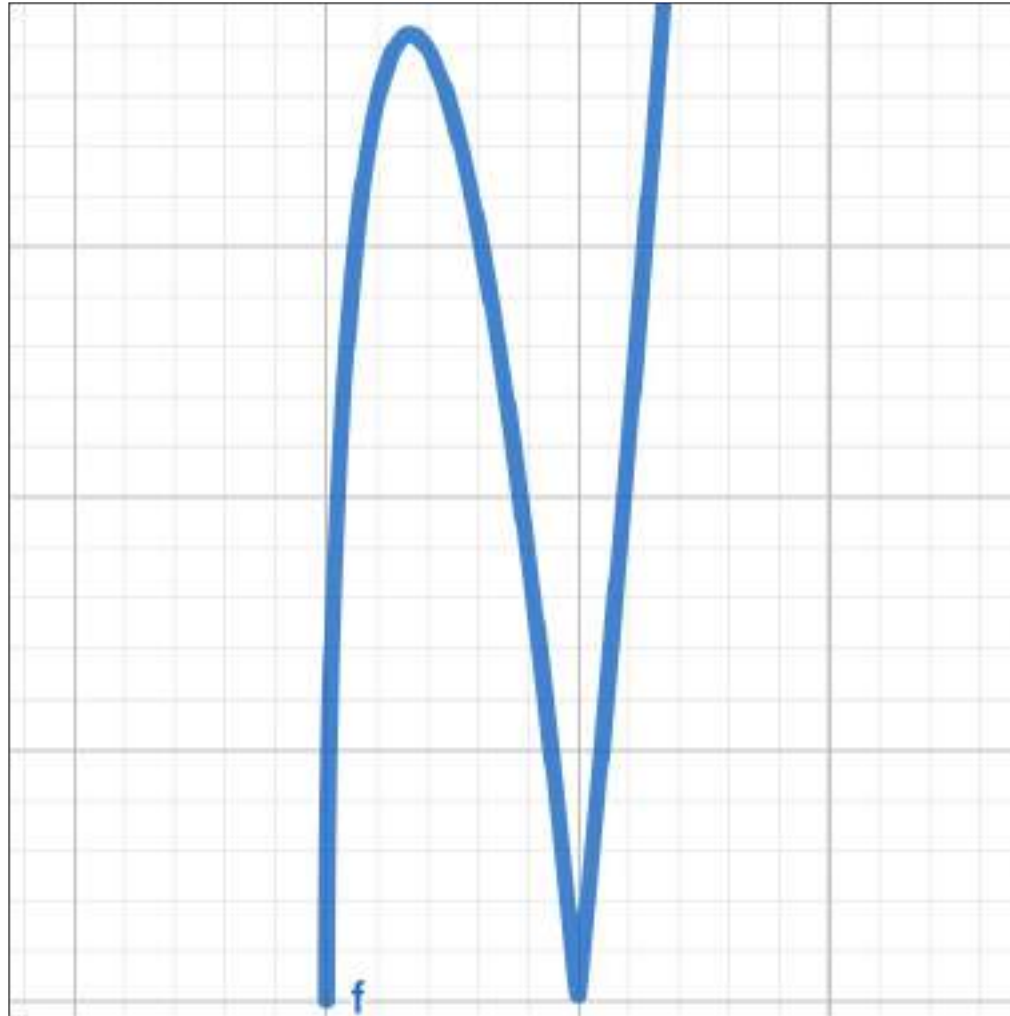
# Elliptical Curve Diffie Hellman

# Elliptical Curve





# Elliptical Curve



## Curve Types

---

x25519

secp256r1

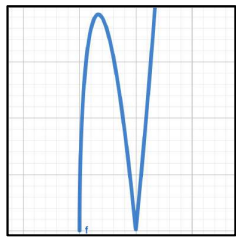
secp284r1

fecp521r1

ffdhe2048

ffdhe3073

# TLS 1.3 ECDHE Key Exchange

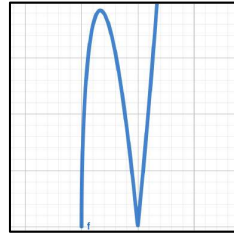


HTTPs Client



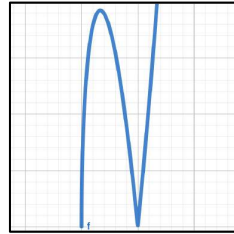
HTTPs Server

# TLS 1.3 ECDHE Key Exchange



HTTPs Client

# TLS 1.3 ECDHE Key Exchange

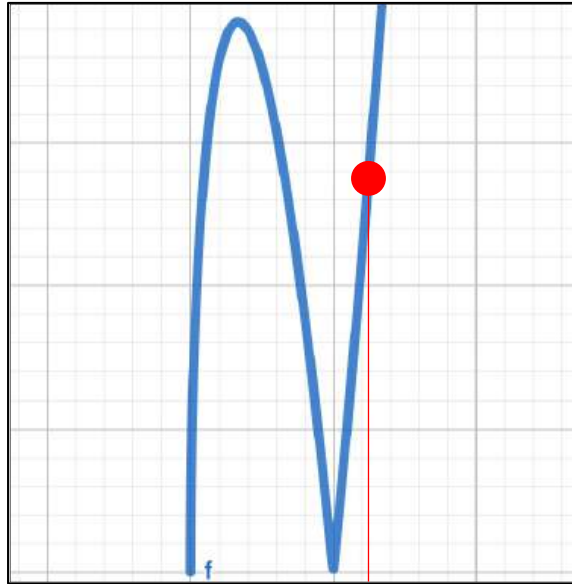


HTTPs Client

Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

# TLS 1.3 ECDHE Key Exchange

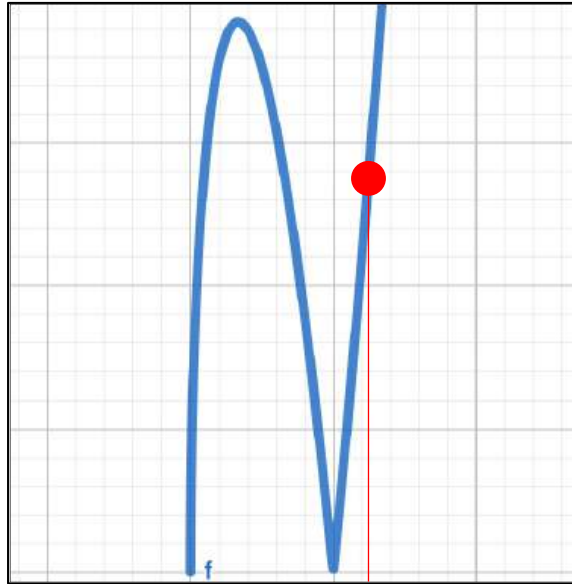


Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

<https://curves.xargs.org>

# TLS 1.3 ECDHE Key Exchange

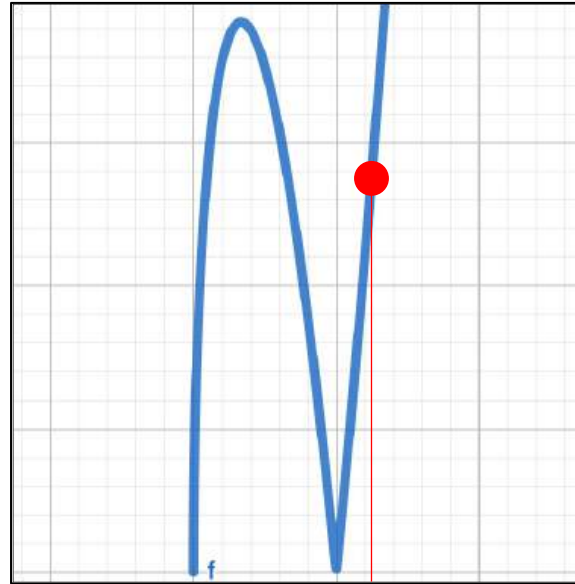


Private Key

af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

<https://curves.xargs.org>

# TLS 1.3 ECDHE Key Exchange



Private Key

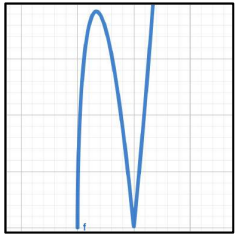
af49806d618a8e0055727d1ea3fcf37776ea990627975a44d43165c09fb82e61

Public Key Share

500fb57e7b13fbaa8fa2630f79481db38c7189ef2ee10ab32797bcf9d8243753

# TLS 1.3 ECDHE Key Exchange

Private  
Key



HTTPs Client



HTTPs Server

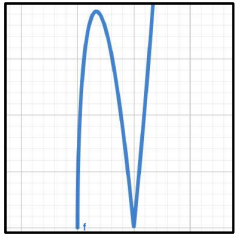
Public  
KeyShare





# TLS 1.3 ECDHE Key Exchange

Private  
Key



HTTPs Client



HTTPs Server

Public  
KeyShare



# TLS 1.3 ECDHE Key Exchange

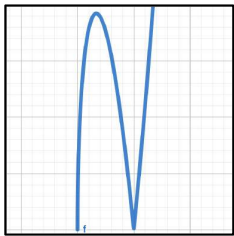


# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange

Private Key

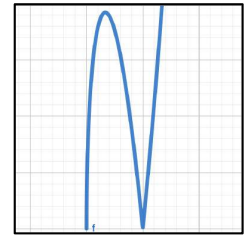


HTTPs Client



Public KeyShare

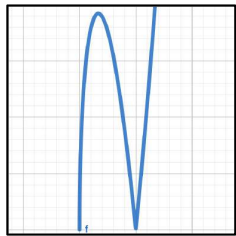
Private Key



HTTPs Server

# TLS 1.3 ECDHE Key Exchange

Private Key



HTTPs Client

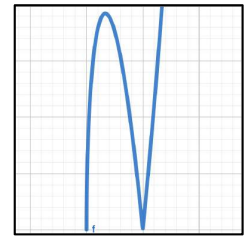


Public KeyShare

Private Key



HTTPs Server

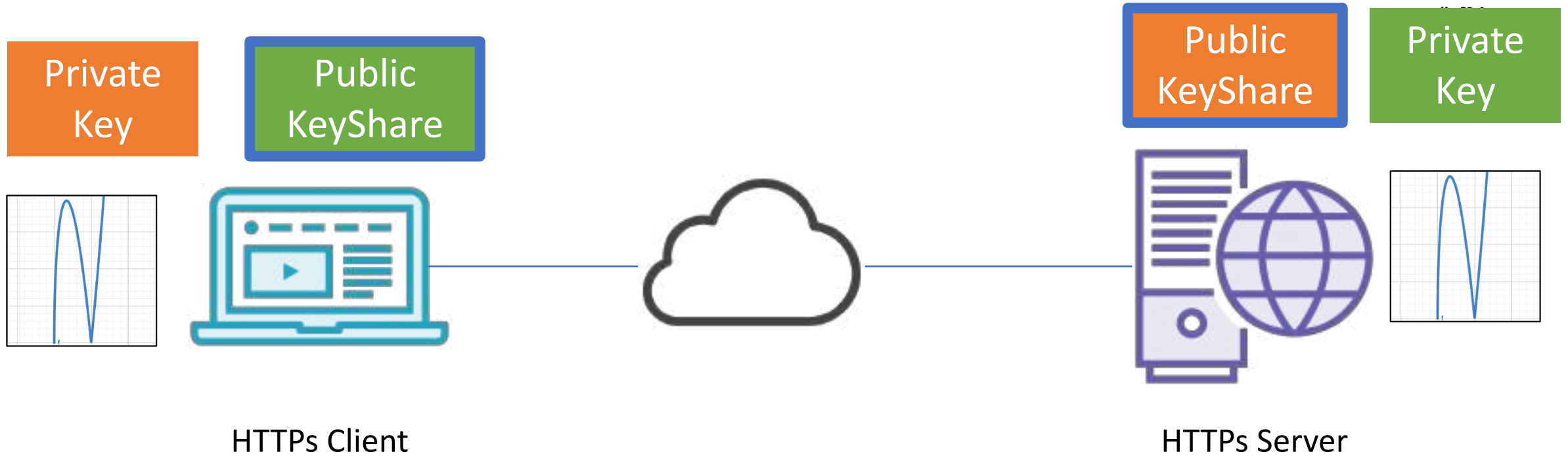


Public KeyShare

# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange

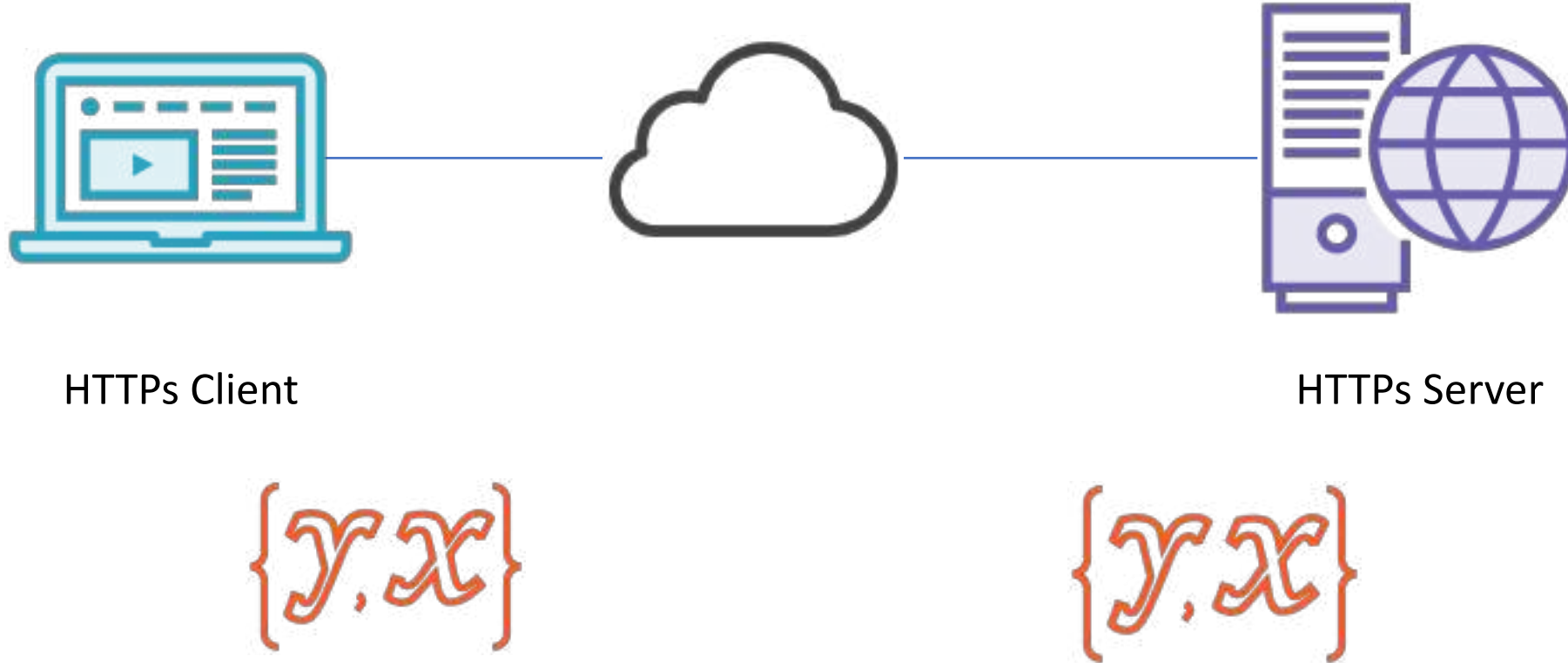


# TLS 1.3 ECDHE Key Exchange





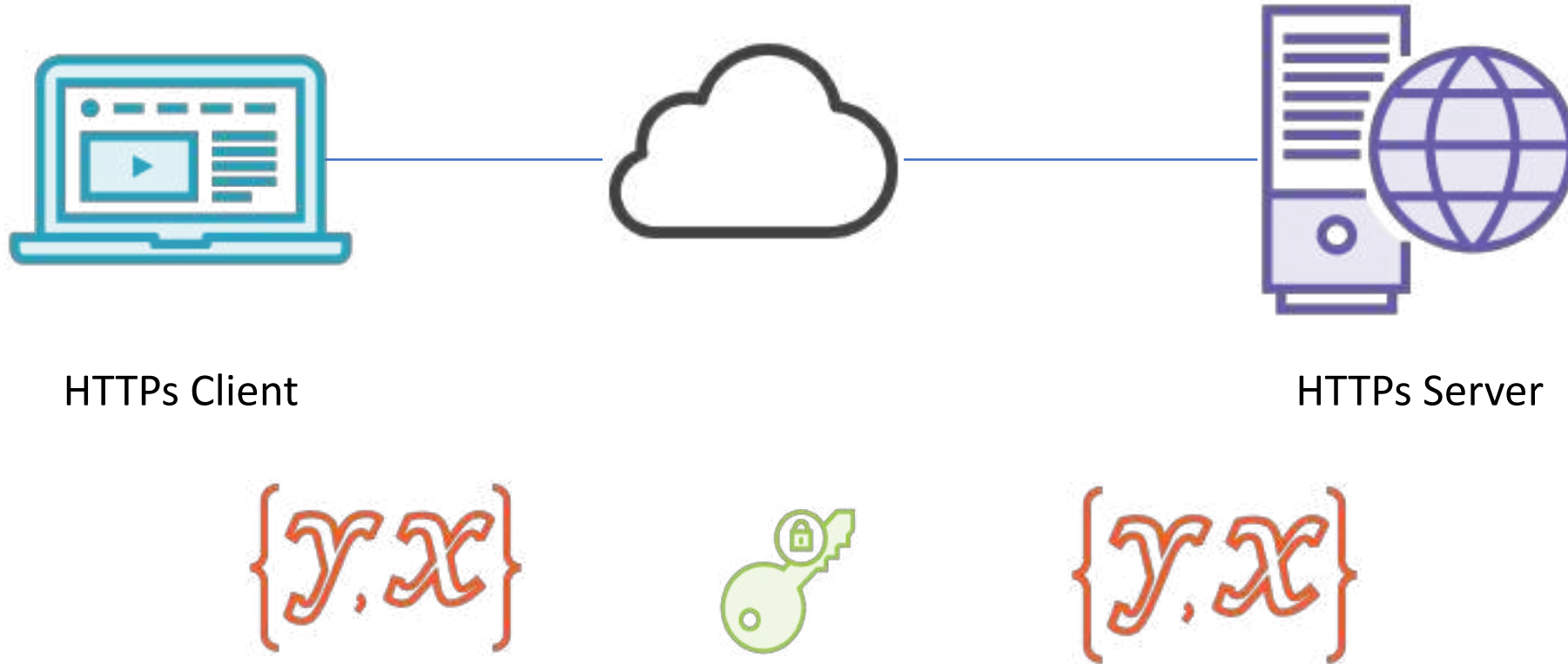
# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



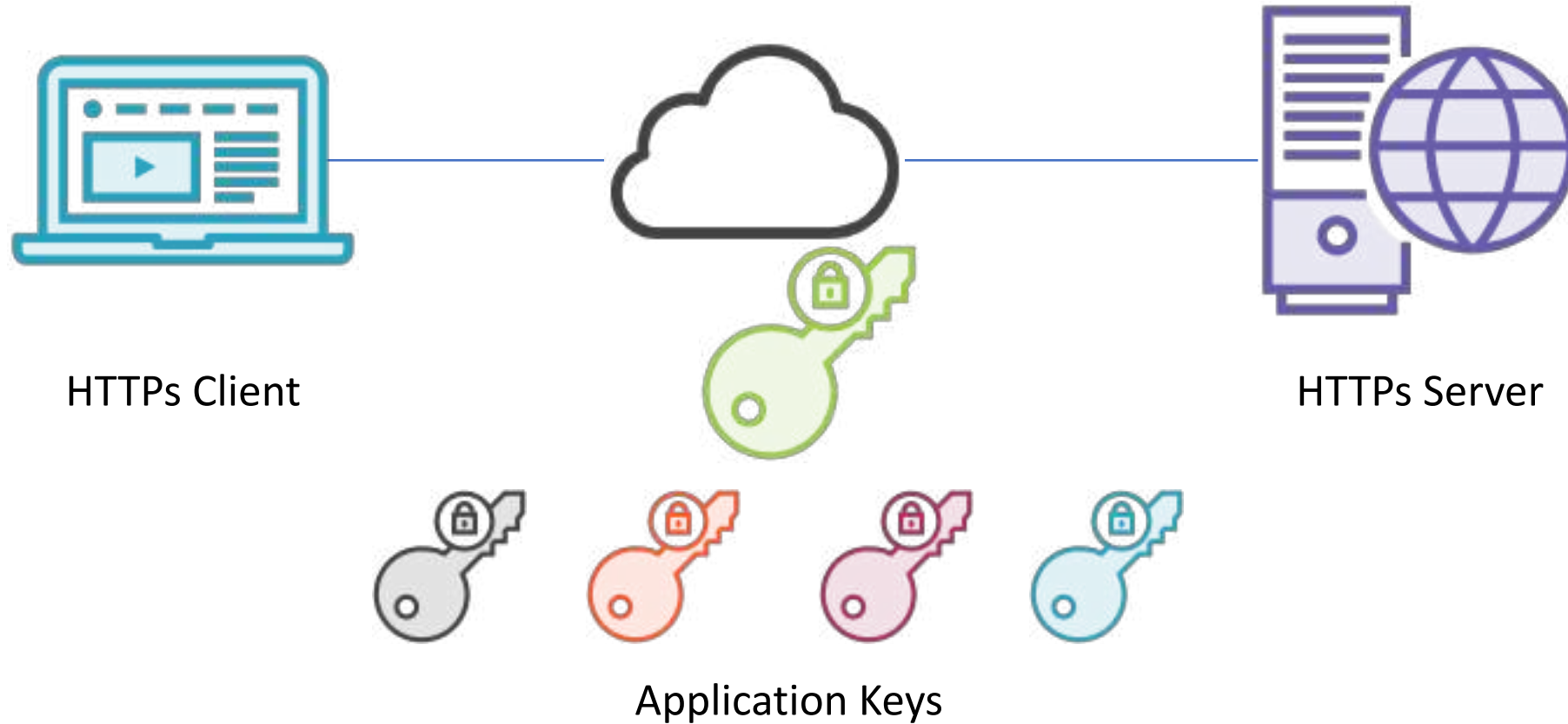
# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



# TLS 1.3 ECDHE Key Exchange



The logo for SharkFest '23 US features a stylized shark fin cutting through a circular blue shape, resembling a globe or a shark's head profile.

**SharkFest'23 US**

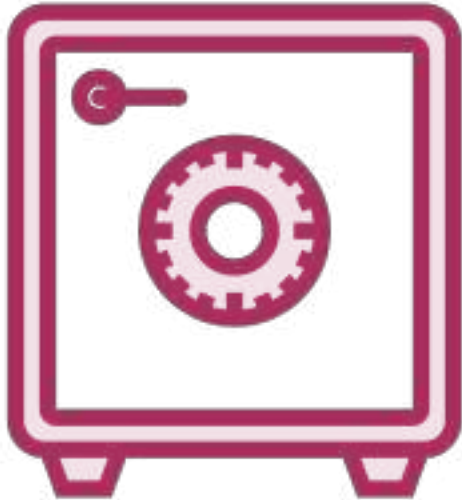
San Diego, CA • June 10-15

#sf23us

# Data Encryption Protocols

# Data Encryption Protocols

## Ciphers



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



Key  
Exchange

Data Encryption

Certificate

# The Design



**Magic Box**



**the Tubes**

# The Design



Key Exchange



Certificate



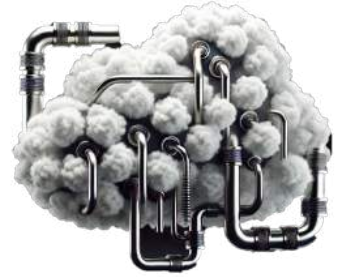
Magic Box

the Tubes

# The Design



**Magic Box**



TLS



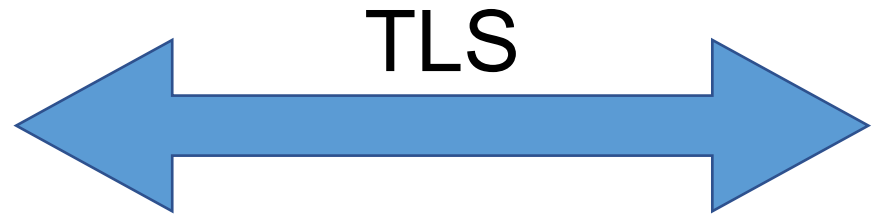
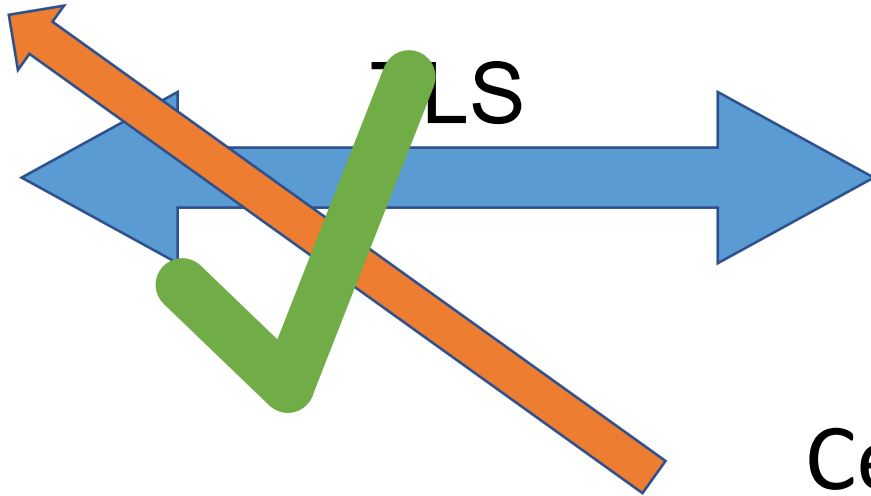
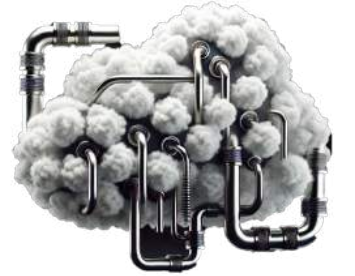
TLS



# The Design



**Magic Box**



Certificate  
Authority



# The Design



**Magic Box**



2 Wireless Adapters

# The Design

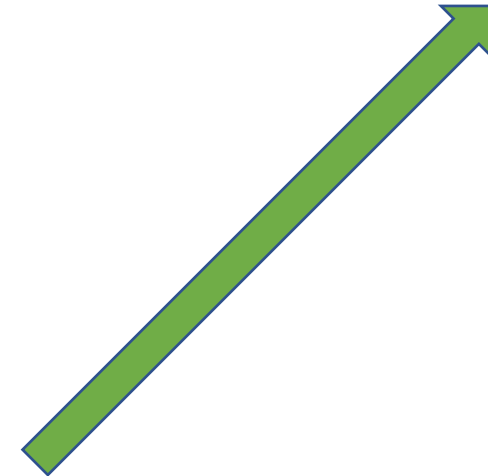


**Magic Box**



2 Wireless Adapters

Wireless NIC 1  
Connect to Local WiFi





# The Design

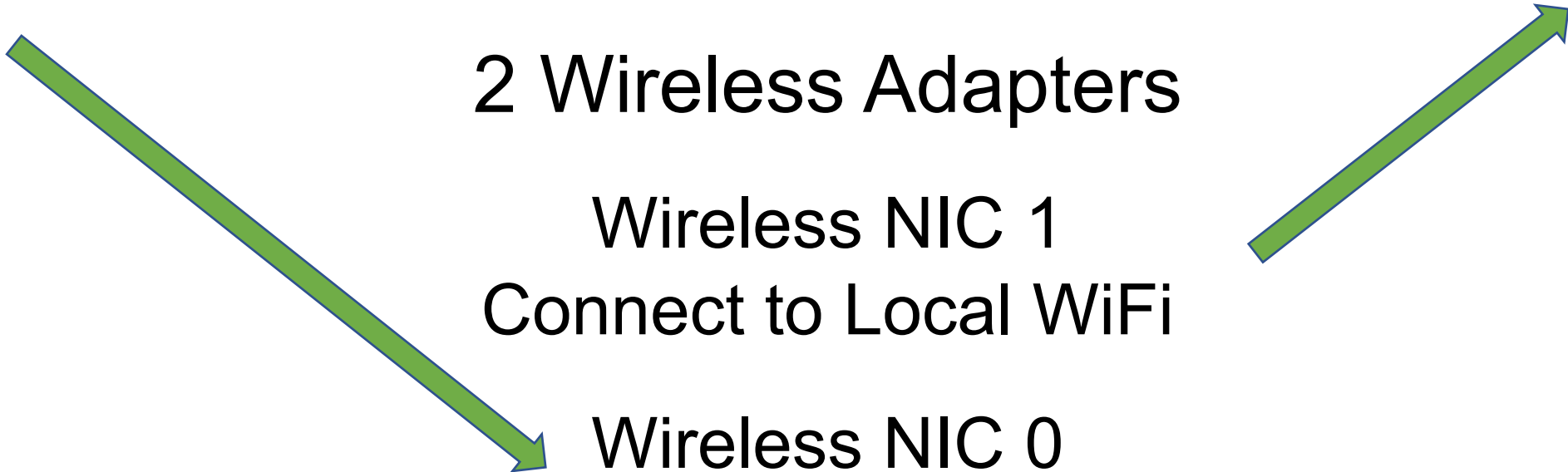


**Magic Box**

2 Wireless Adapters

Wireless NIC 1  
Connect to Local WiFi

Wireless NIC 0  
Access Point



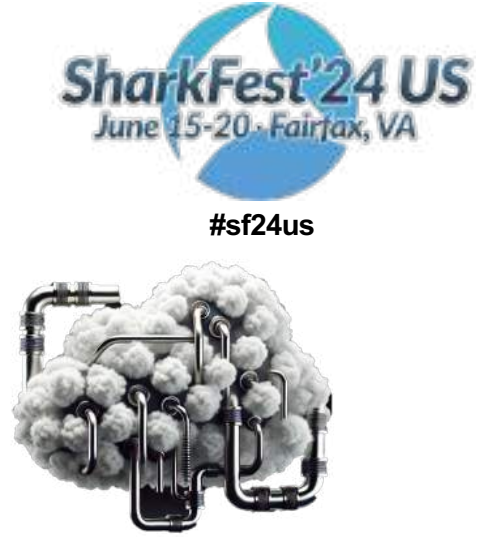


# The Design



**Magic Box**

2 Wireless  
Adapters



Service to create  
Access Point  
HostAPD

# The Design



**Magic Box**



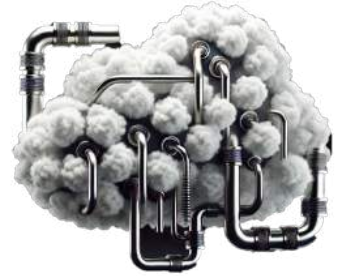
2 Wireless  
Adapters

HostAPD  
DNSmasq

# The Design



**Magic Box**



2 Wireless  
Adapters

HostAPD  
DNSmasq





WIRESHARK  
WIRELESS NETWORKING

40 TOWER  
PT-2

WIRESHARK

OCEAN  
HARD

WICKET HEAD

PULL









Fest'24 US  
-20 - Fairfax, VA

#sf24us



**SharkFest'24 US**  
June 15-20 - Fairfax, VA

#sf24us

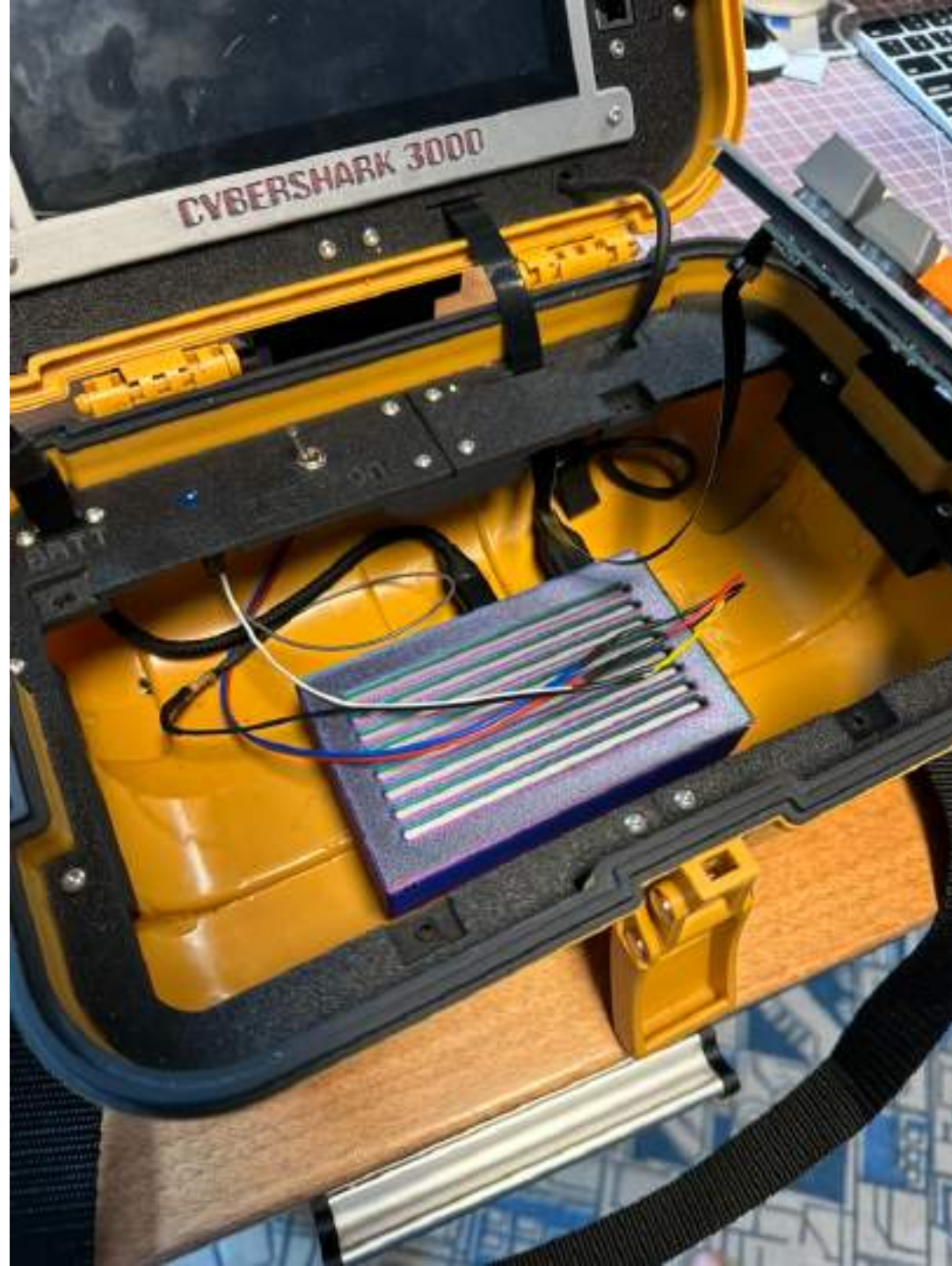




sfFest'24 US  
5-20 - Fairfax, VA

#sf24us





**SharkFest'24 US**  
June 15-20 - Fairfax, VA

#sf24us

# Hardware Build

Raspberry Pi 4 – 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>