

How HTTPS:// Works !!

SECURE

* Data transfer between Client & Server is encrypted.

What

is

HTTP ?
Hyper Text Transfer Protocol



A Standard way to
Share Hyper Text
on Internet



Q But without common encryption Key, how data is encrypted ??

A Let's see how...

1 Server Certificate Check

Client



CLIENT: HELLO

SERVER: HELLO

SERVER
CERTIFICATE

Is this valid?

YES

Server



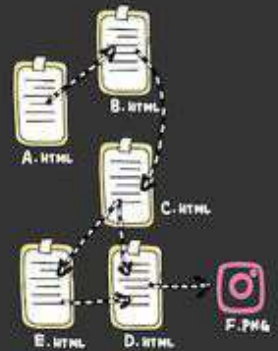
Certificate
Certifying
Authority



Server



Hyper Text : A Document / text that Contains Links to other text.
Eg HTML Pages.



3

Encrypted Tunnel
for data transmission

2 Key Exchange

Client



Extract Server
From

Creates a
Session Key

I know A, B, C, D cipher
Suites

OK, Lets use "C"
cipher suite

Encrypt using
Server & "C" cipher suite

Server



Decrypt
using

* At this point
Server has

Client



At this point
Client and Server
both have common
Key, Also Known as
Session Key

Encrypt data
with Session Key

Decrypt data
with Session Key

Decrypt data
with Session Key

Encrypt data
with Session Key

Server



@ Sec_10

ByteByteGo