WHAT IS

SSL

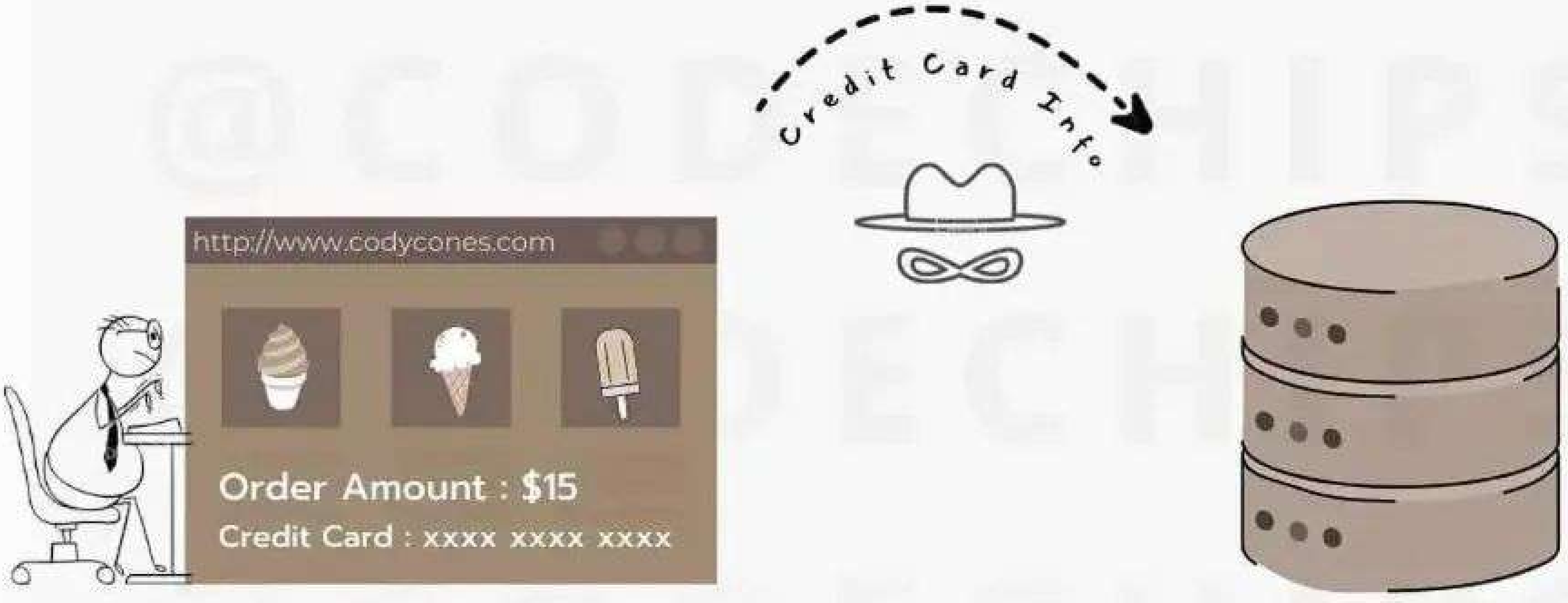
@codechips

Art Credit : @william_silva226

So you are having your Ice Cream Website where customers can order their desserts

http://www.codycones.com

But what if someone interprets your customers personal data



http://www.codycones.com

Order Amount : $15

Credit Card : xxxx xxxx xxxx

That is why it is necessary to have an **SSL**

httpS://www.codycones.com

SSL stands for **Secure Sockets Layer**

SSL is a secure protocol developed for sending information securely over the Internet

It helps to create an encrypted connection between the device of the visitor and your website

Encrypted Credit Card Info
http://www.codycones.com
I can't read the data

Order Amount : $15

Credit Card : xxxx xxxx xxxx

You must first have an SSL Certificate

An **SSL certificate** is a digital certificate or data file that verifies the owner or authenticity of a website

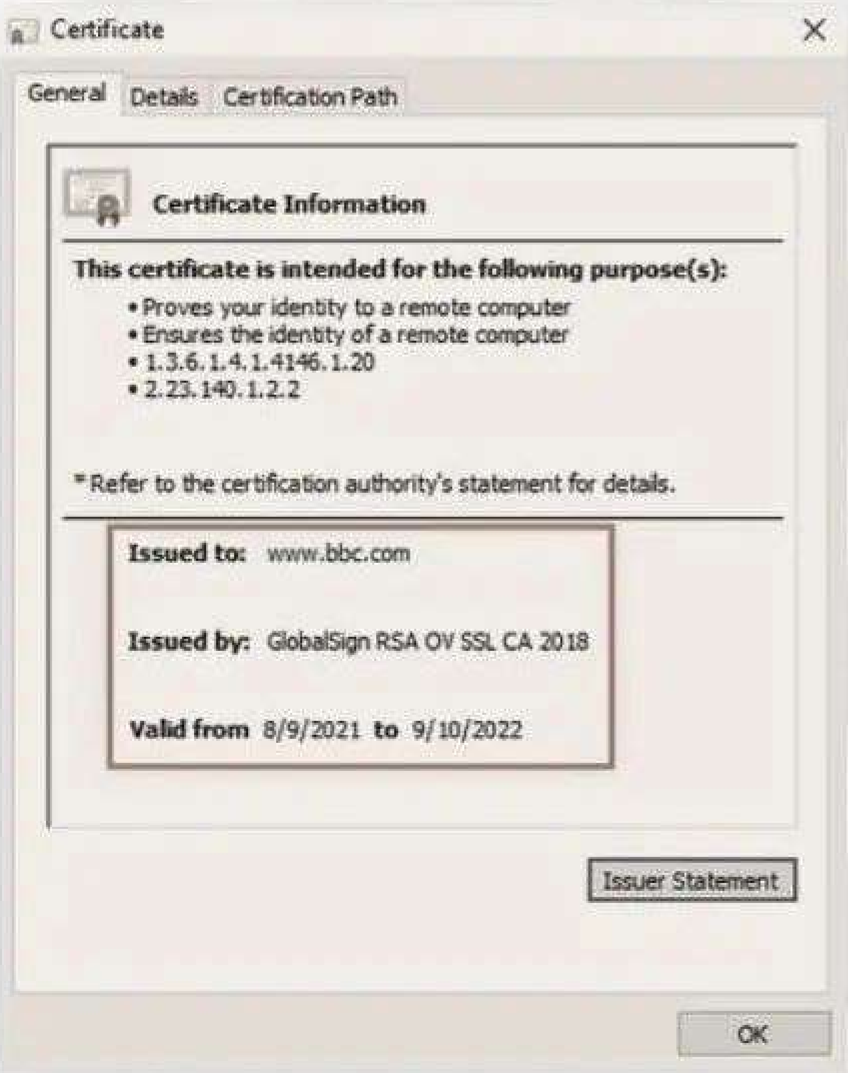
A CA is an outside organization, a trusted third party, that generates and gives out SSL certificates

An SSL Certificate consists of :

issued to

issued by

public key



Certificate Information

This certificate is intended for the following purpose(s):

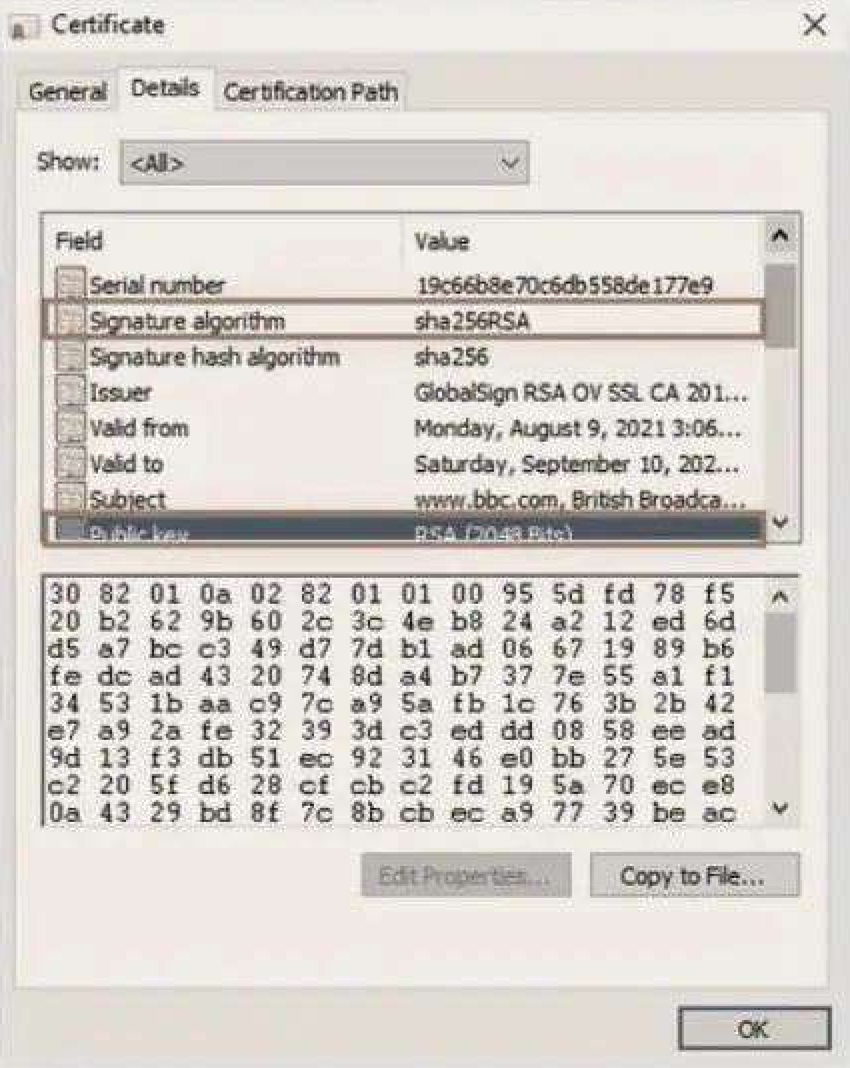
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 1.3.6.1.4.1.4146.1.20
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: www.bbc.com

Issued by: GlobalSign RSA OV SSL CA 2018

Valid from 8/9/2021 **to** 9/10/2022



Show: <All>

Field	Value
Serial number	19c66b8e70c6db558de177e9
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	GlobalSign RSA OV SSL CA 201...
Valid from	Monday, August 9, 2021 3:06...
Valid to	Saturday, September 10, 202...
Subject	www.bbc.com, British Broadca...
Public key	RSA (2048 Bits)

```
30 82 01 0a 02 82 01 01 00 95 5d fd 78 f5
20 b2 62 9b 60 2c 3c 4e b8 24 a2 12 ed 6d
d5 a7 bc c3 49 d7 7d b1 ad 06 67 19 89 b6
fe dc ad 43 20 74 8d a4 b7 37 7e 55 a1 f1
34 53 1b aa c9 7c a9 5a fb 1c 76 3b 2b 42
e7 a9 2a fe 32 39 3d c3 ed dd 08 58 ee ad
9d 13 f3 db 51 ec 92 31 46 e0 bb 27 5e 53
c2 20 5f d6 28 cf cb c2 fd 19 5a 70 ec e8
0a 43 29 bd 8f 7c 8b cb ec a9 77 39 be ac
```

validity period

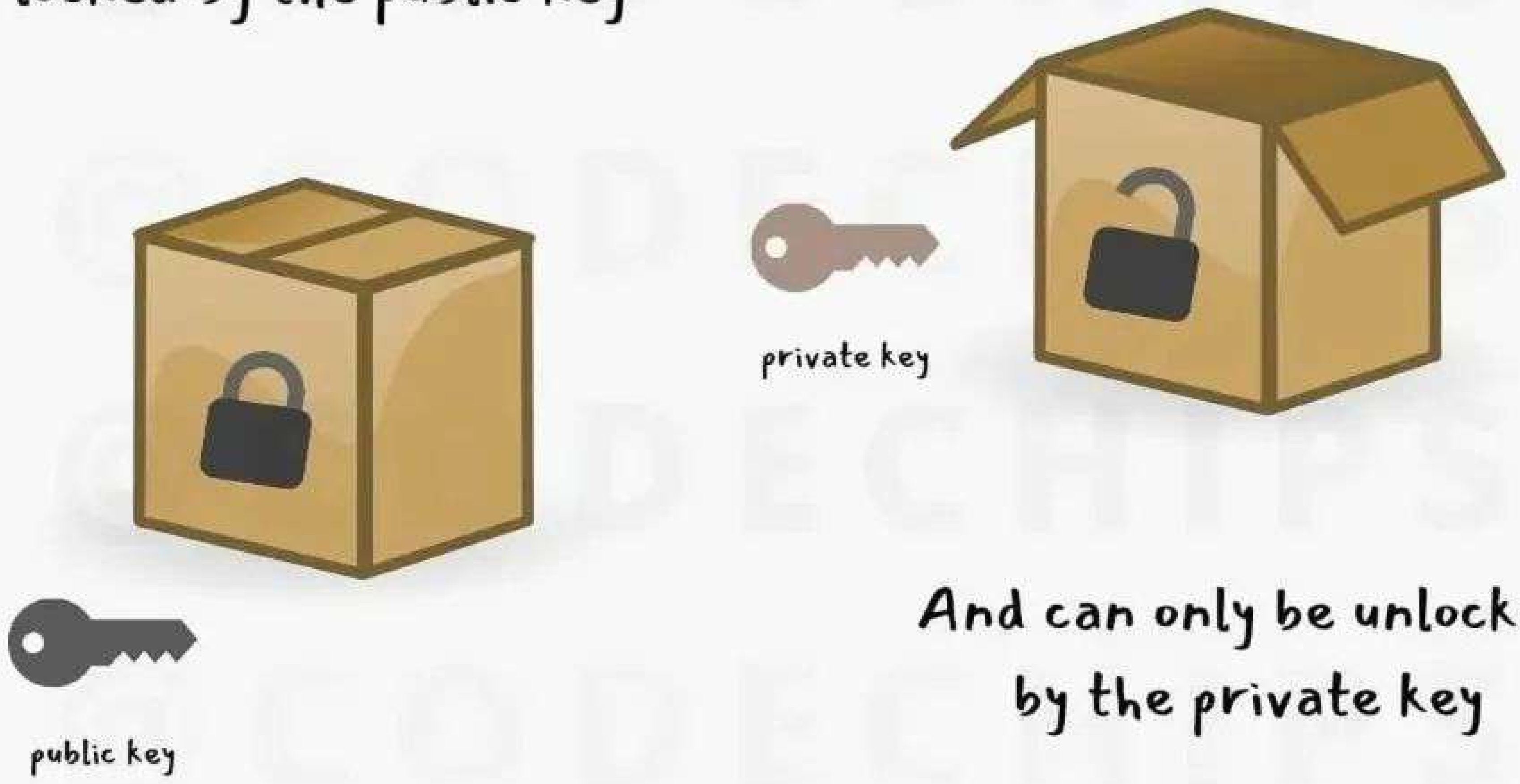
serial number

CA's digital signature

How SSL protocol works ?

Think of a box with 2 keys :
Public Key and **Private** Key

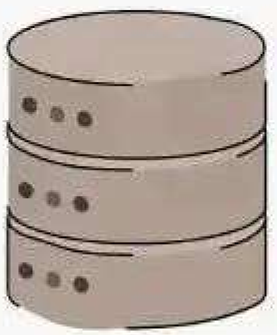
This box can only be locked by the public key



And can only be unlocked by the private key

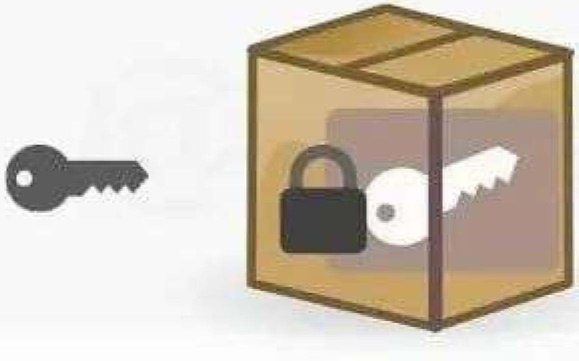
Now when the user visits codycones.com

http://www.codycones.com
Order Amount : $15
Credit Card : xxxx xxxx xxxx



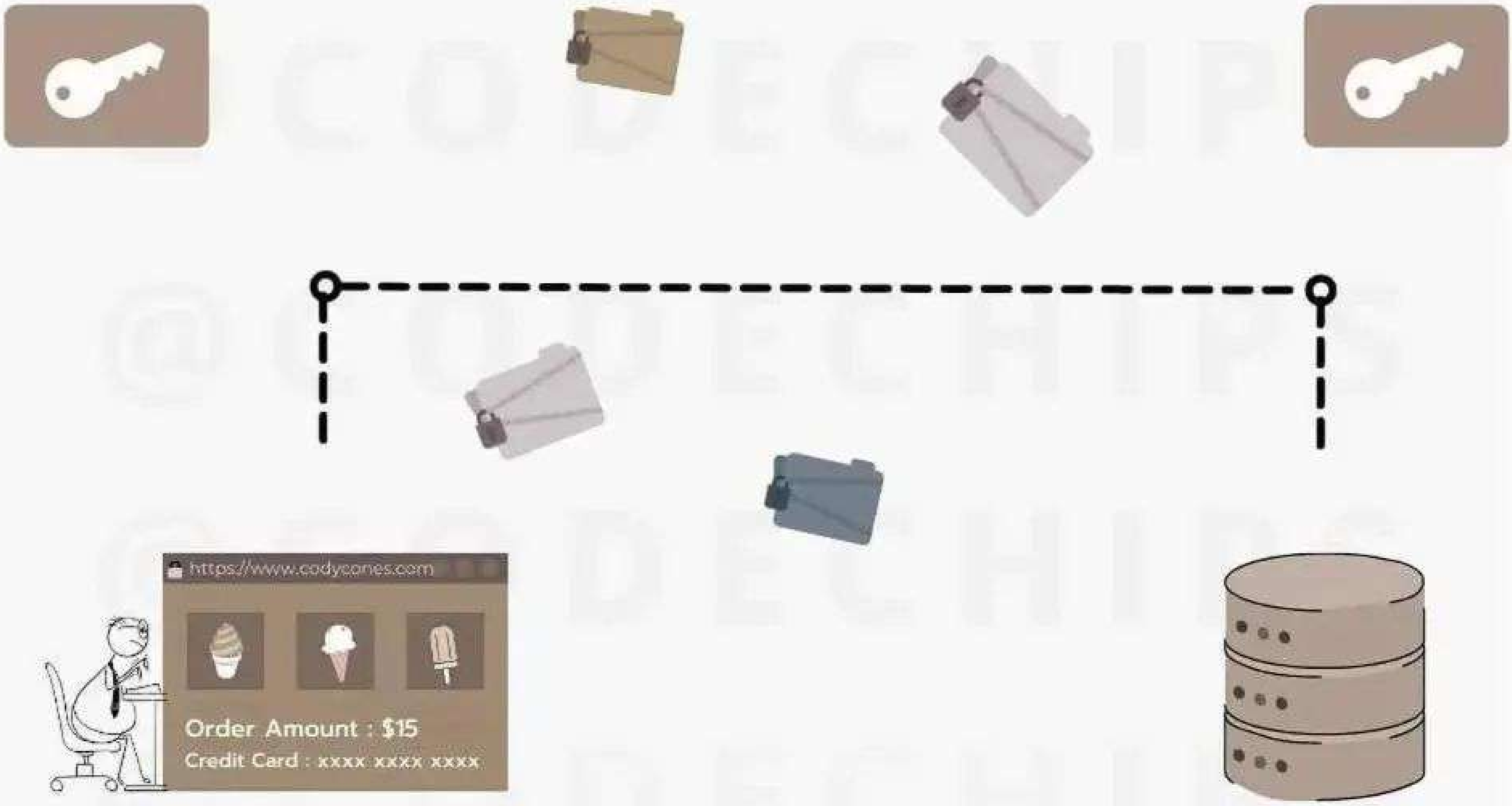
Server responds with SSL certificate along with Public Key

Now the browser sends the **session key** in a box and locks it with the public key sent



This box is unlocked with the private key to acquire the symmetric session key

The client and the server now use a shared session key to **encrypt** and **decrypt** actual data and transfer it



Order Amount : $15

Credit Card : xxxx xxxx xxxx