邓哥

摸尼卡

成哥

邓哥

我爱你

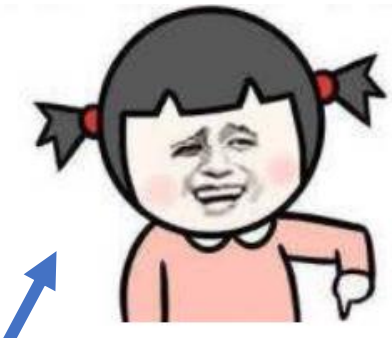
摸尼卡

邓哥

我爱你

成哥

我恨你

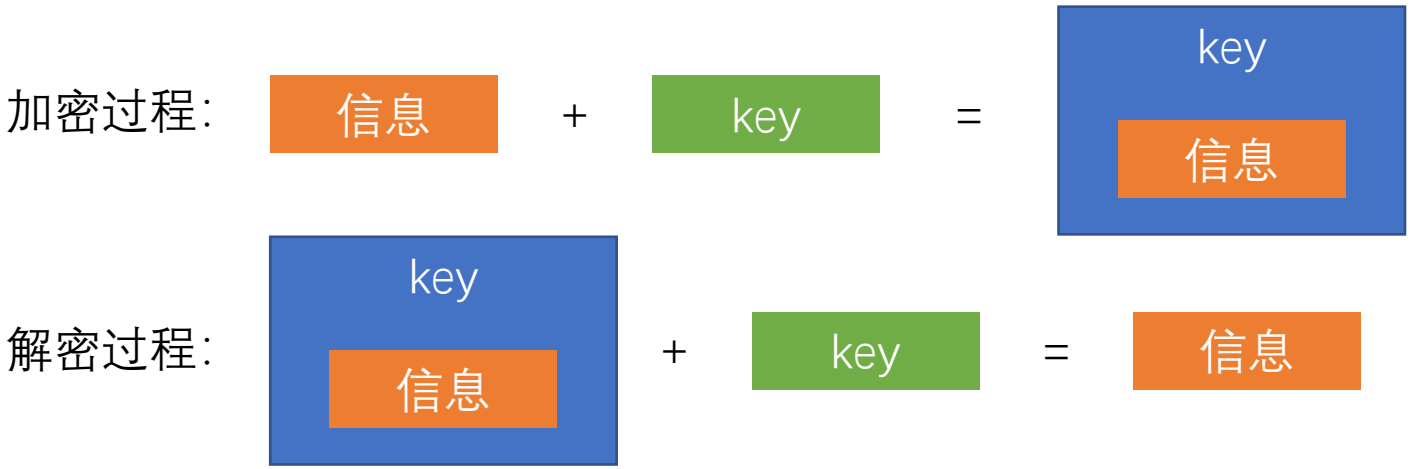


摸尼卡

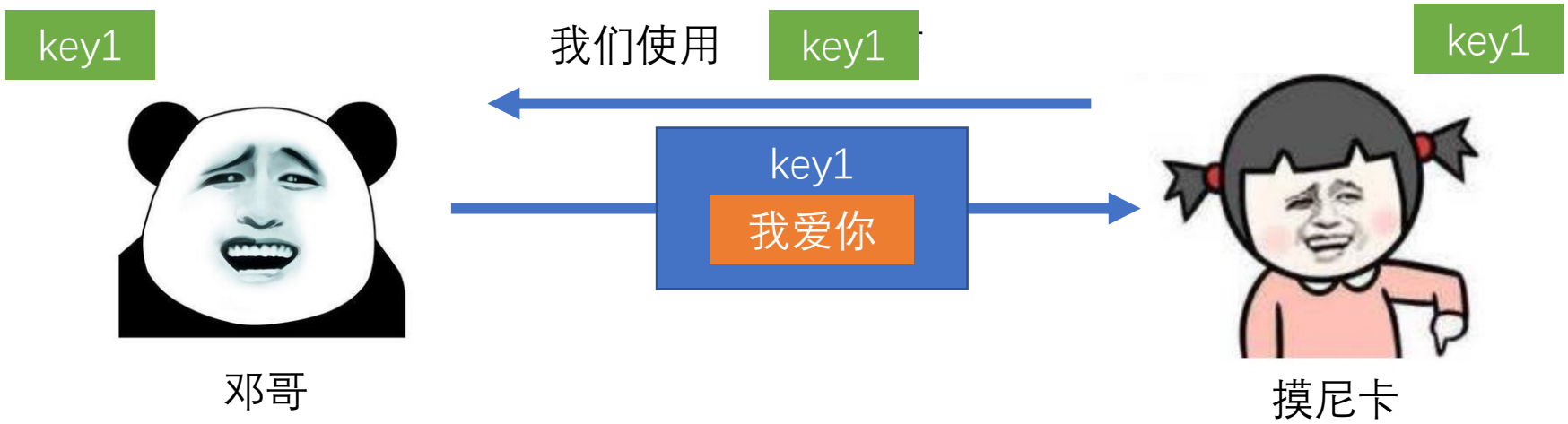
加密

加密

对称加密：产生一个密钥，可以用其加密，也可以用其解密



常用算法：DES、3DES、AES、Blowfish等


key1
我们使用
key1
key1
key1
我爱你
邓哥
摸尼卡

key1

邓哥

key1

摸尼卡

我们使用 key1 言

我们使用 key1 言

key1

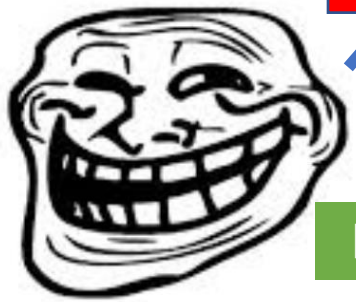
成哥

key1

邓哥

key1

我爱你



成哥

key1

key1

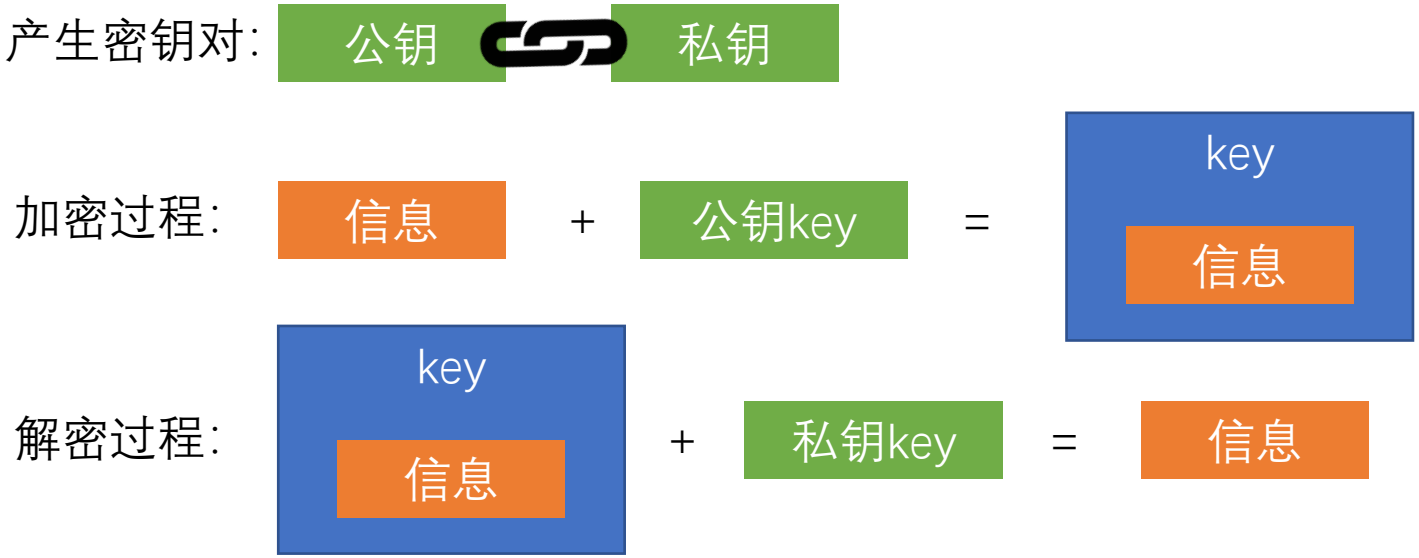
我恨你

key1

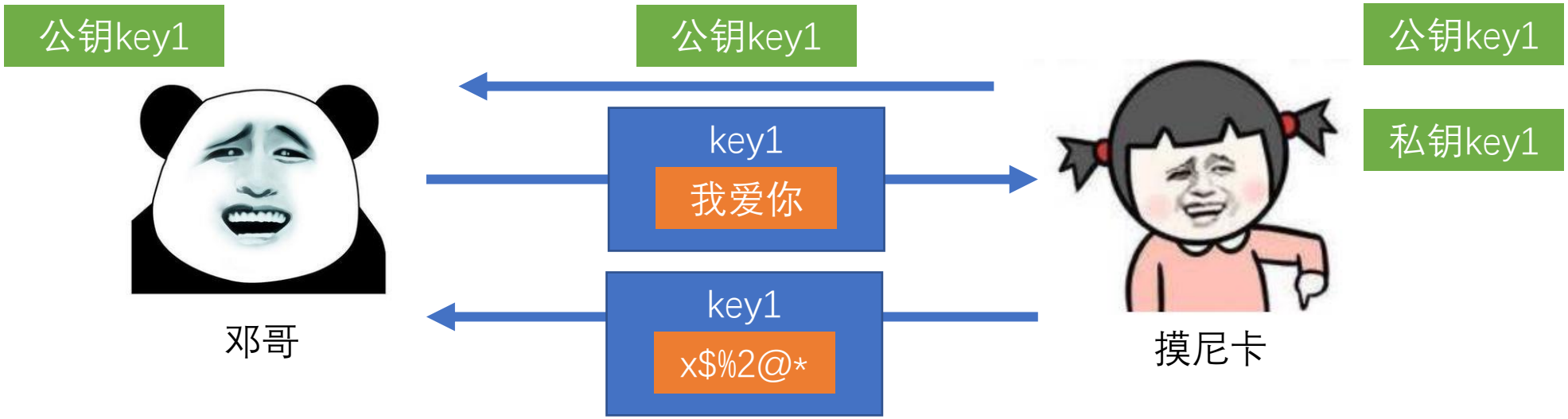
摸尼卡

加密

非对称加密：产生一对密钥，一个用于加密，一个用于解密



常用算法：RSA、Elgamal、Rabin、D-H、ECC等


公钥key1
公钥key1
公钥key1
私钥key1
key1
我爱你
key1
x$%2@*
邓哥
摸尼卡

公钥key1

key2

邓哥

公钥key1

key1

key2

key2

我爱你

key2

你是个好人

公钥key1

私钥key1

key2

摸尼卡

公钥key3

邓哥

公钥key1

私钥key1

摸尼卡

公钥key3

公钥key1

成哥

公钥key1

公钥key3

私钥key3

公钥key3

key2

邓哥

key3

key2

成哥

key1

key2

公钥key1

公钥key3

私钥key3

key2

摸尼卡

公钥key1

私钥key1

key2

公钥key3

key2

邓哥

key2

我爱你

成哥

公钥key1

公钥key3

私钥key3

key2

key2

我恨你

摸尼卡

公钥key1

私钥key1

key2

CA：Certificate Authority
证书颁发机构

证书颁发流程

服务器地址：www.monica.com

摸尼卡

公钥key1

公钥 KEY

私钥 KEY

证书 Digital Certificate (DC)

由于证书中的服务器公钥、证书签名是通过CA的私钥加密的

因此，其他终端只能通过CA的公钥解密读取，但无法重新加密伪造

证书签名 Signature

证书签名 = www.monica.com + CA公钥 KEY + 公钥key1

证书签名的算法是公开的，它出现的目的，是为了让每一个拿到证书的终端，可以验证签名是否被篡改

第1步：浏览器获取证书

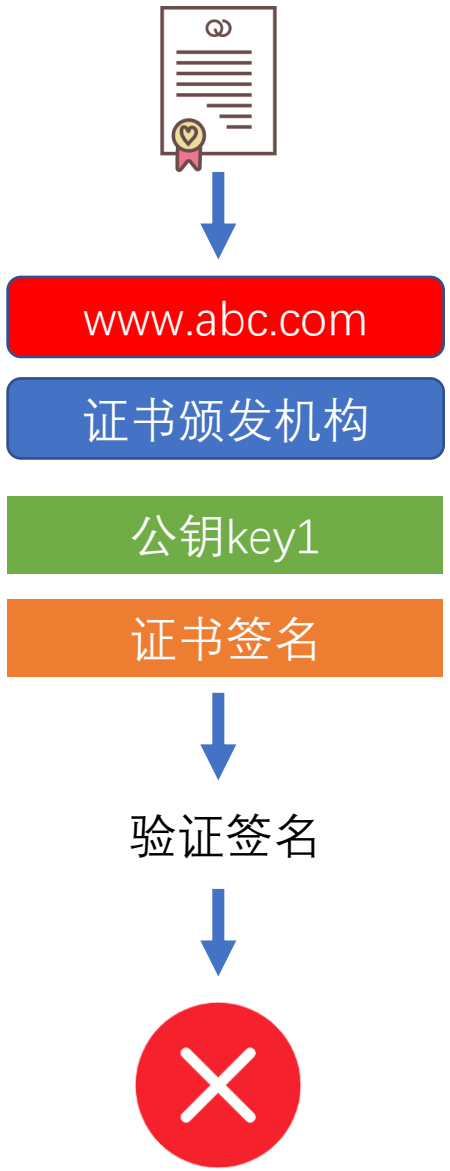
邓哥

摸尼卡

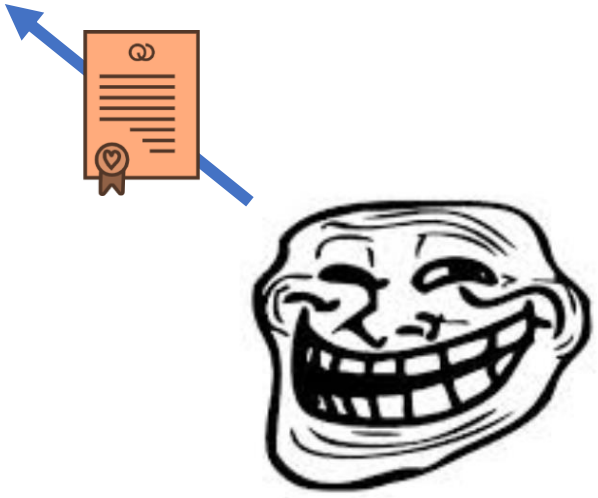
公钥key1

私钥key1

第1步：无法被篡改



邓哥



成哥

摸尼卡

公钥key1

私钥key1

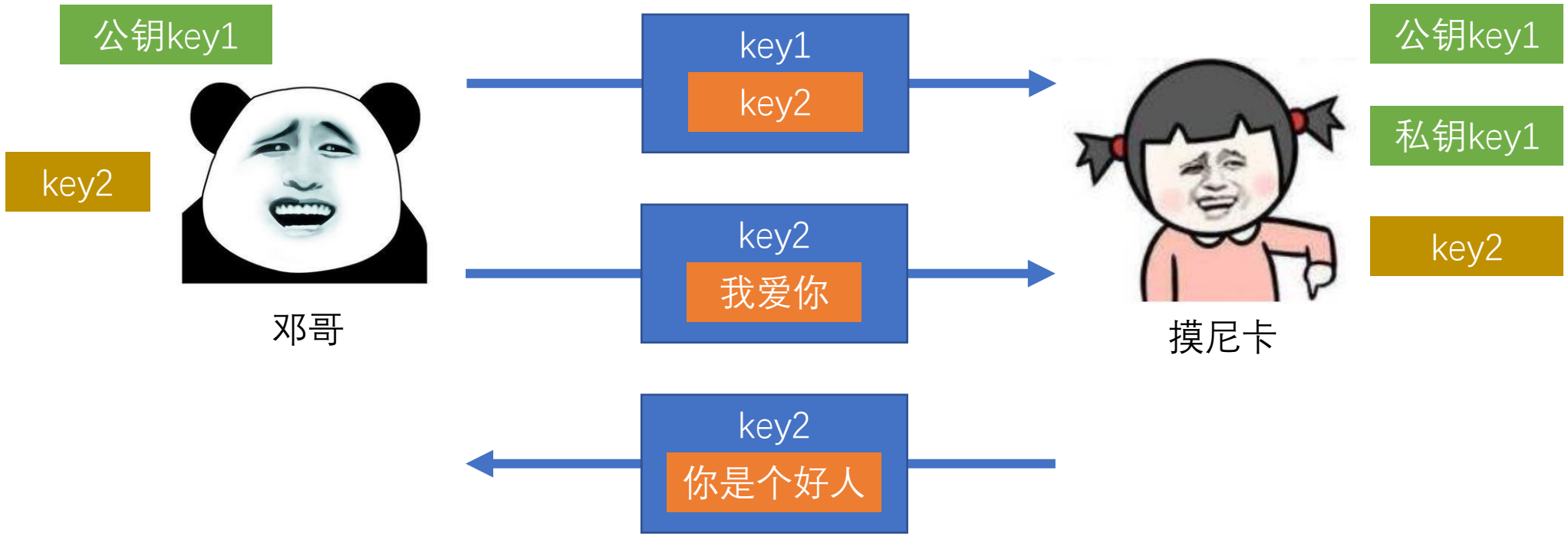
www.monica.com

证书颁发机构

公钥key1

证书签名

后续：和之前一样


公钥key1
key2
邓哥
key1
key2
key2
我爱你
key2
你是个好人
摸尼卡
公钥key1
私钥key1
key2

后续：第三方无法查看和篡改

公钥key1

key2

邓哥

key1

key2

成哥

key1

key2

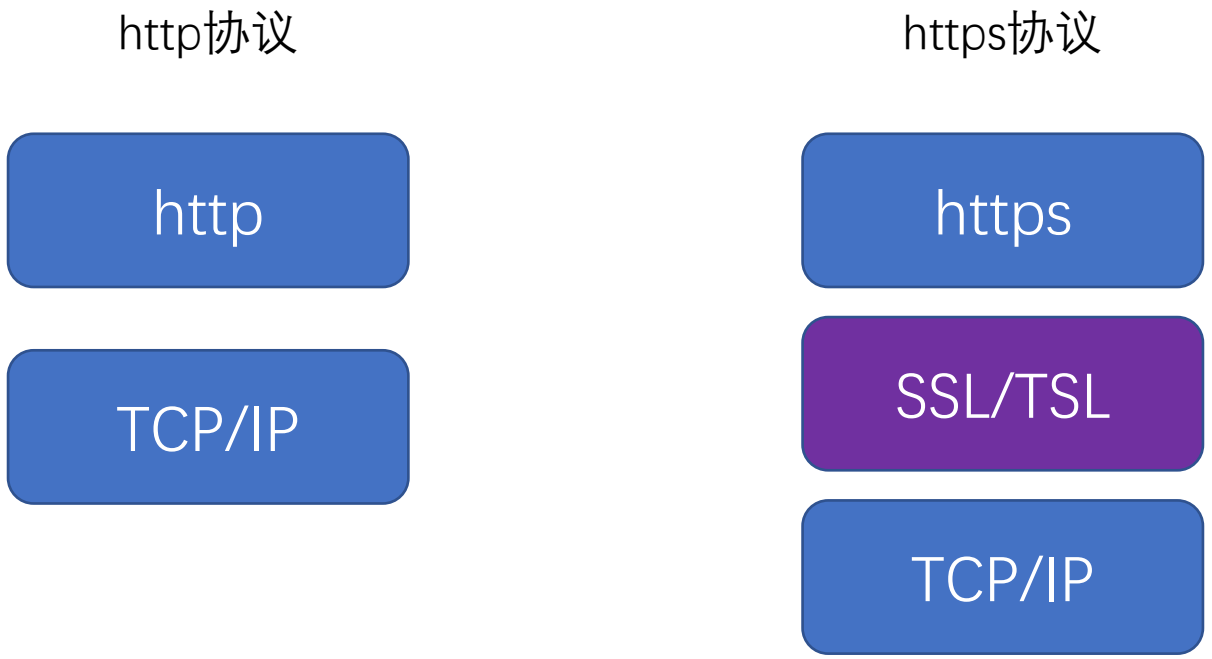
公钥key1

摸尼卡

公钥key1

私钥key1

key2



浏览器希望，通过https协议拿到的网页中，其他资源均应该使用https协议获取

服务器：申请证书

客户端：访问时，使用 https://xxxx

https的默认端口是443