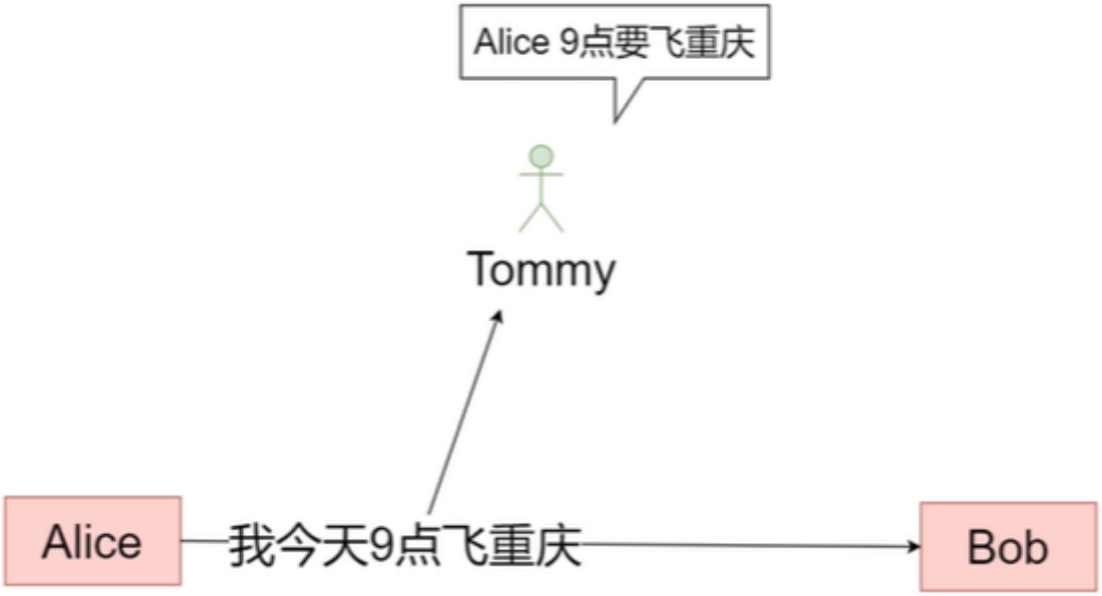
课程目标

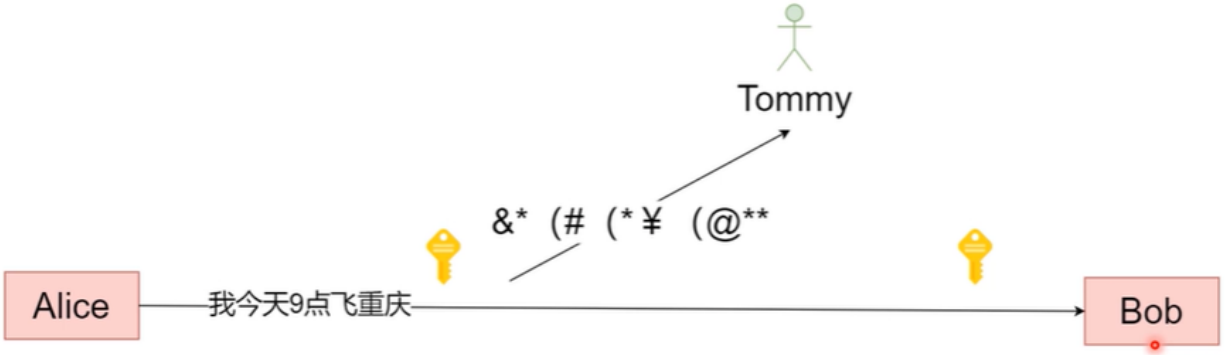
对称加密和非对称加密

明文传输



Alice发给Bob明文信息，说我今天9点去重庆,Tommy是黑客，正好是小区交换机的工作人员，看到这个明文信息之后，接下来就动坏心思了。

加密



Alice 把消息加密,送给Bob,但是同时 Bob拿到消息之后得进行解密，这样即使中间Tommy看到消息也是一串加密后得字符，这时候，对于Tommy来说，这一串数字并没啥用。

什么是加密

将明文信息变成不可读的密文内容,只拥有解密方法的对象才能够将密文还原成加密前的内容

KGDEINPKLRIJLFGOKLMNISOJNTVWG

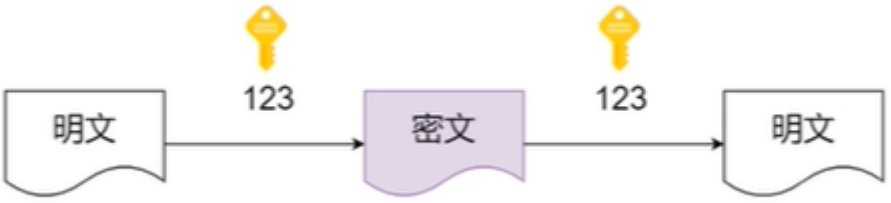
KGDEINPKLRIJLFGOKLMNISOJNTVWG

加密方法/解密方法

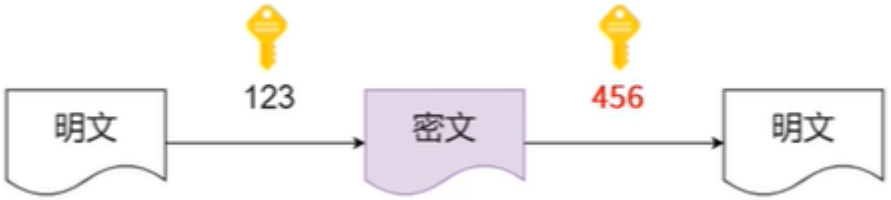
- 计算机中，加密和解密方法，可以描述一段程序,我们称作加密/解密算法
- 加密解密有时候会对暗号,比如上个例子每次跳动三个字符,[3]就是一个暗号,这个我们称作[秘钥]，通过这个[秘钥]加密成密文，也可以通过这个[秘钥]得到明文。但是这个秘钥不一定是同一个。下面对称和非对称加密可以说明。

对称加密/非对称加密

- 加密和解密的暗号(秘钥)相同，我称为对称加密。 **(通讯加密解密用的同一把钥匙)**

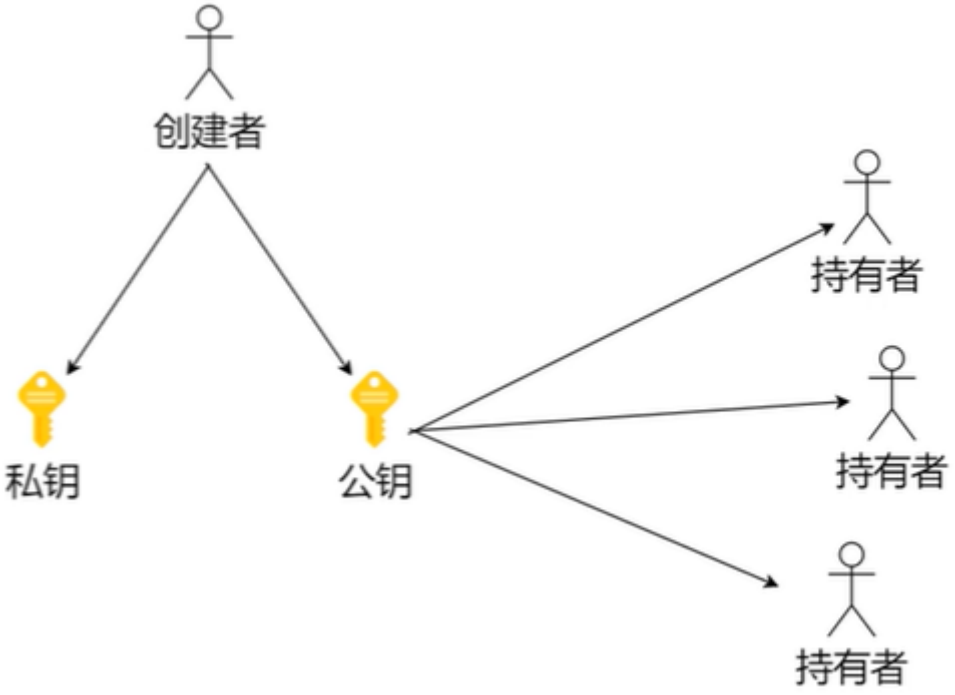


- 加密和解密的暗号(秘钥)不同，我称为非对称加密。**(通讯加密解密用的不同的钥匙)**



非对称加密(秘钥对，公私钥体系)

创建者创建一个秘钥对(分成公钥和私钥)，公私钥体系中，公钥加密必须私钥解密，私钥加密必须公钥解密，创建者保留私钥，公钥向外界公开。每个钥匙只能做一件事情，这就是非对称加密。例如：淘宝，所有人跟淘宝通讯的时候都持有公钥，淘宝自己持有私钥。



思考

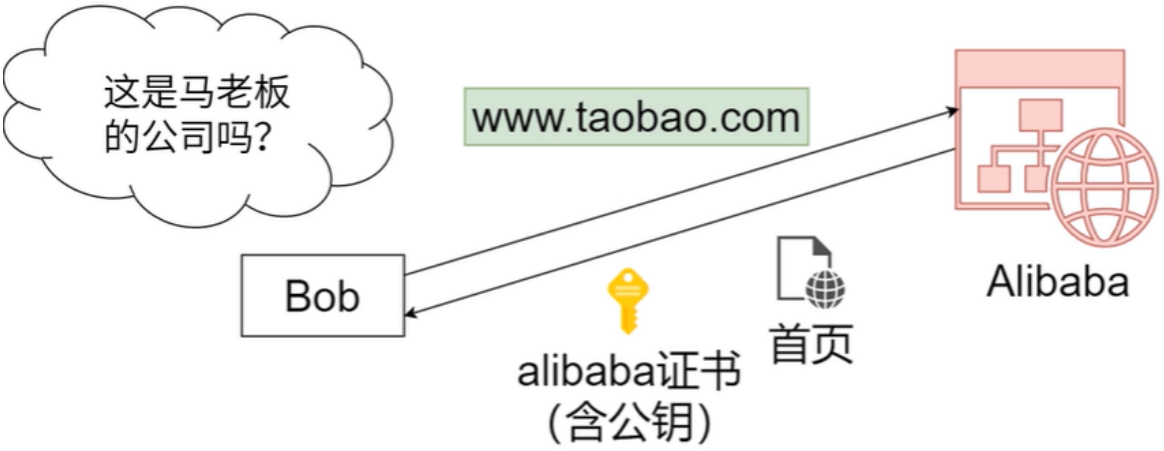
- 为什么加密解密可以不用一把钥匙？(这个是数学算法的层面了，程序员暂时不考虑这个，可以看需要，数学家用一个数字加密，然后用另外一个数字解密等相关文章)
- 什么场景需要非对称加密？不放心对方保管秘钥的情况，比如:你是淘宝，小明和小红都来你这里购物，你为了通讯安全，如果你使用对称加密 ，你把钥匙复制很多份，给小明一份，给小红一份，自己保留一份，你和小明的通信，小红也可以看

到，因为小红有相同的钥匙。这样就非常不安全。你又想每个用户都要发一把钥匙，然后自己保留一把钥匙和每个用户一一对应，每创建一个用户都用创建一把钥匙，这个也是不现实的。所以，这时候公私钥体系就派上用场了，淘宝做了两把钥匙，公私给用户，私钥留给自己，淘宝给到用户的一些公用数据是对公的，每个用户都可以看到，如果商品列表。但是每个用户发送给淘宝的可能就不一样了，需要用户登录，输入密码，提交订单信息，银行卡账号这些私密隐私信息，并且需要用户自己的公钥加密，只是淘宝的私钥才能解密(除非偷到淘宝的私钥，这也不太现实)，非对称加密会更加安全。

解决信任问题

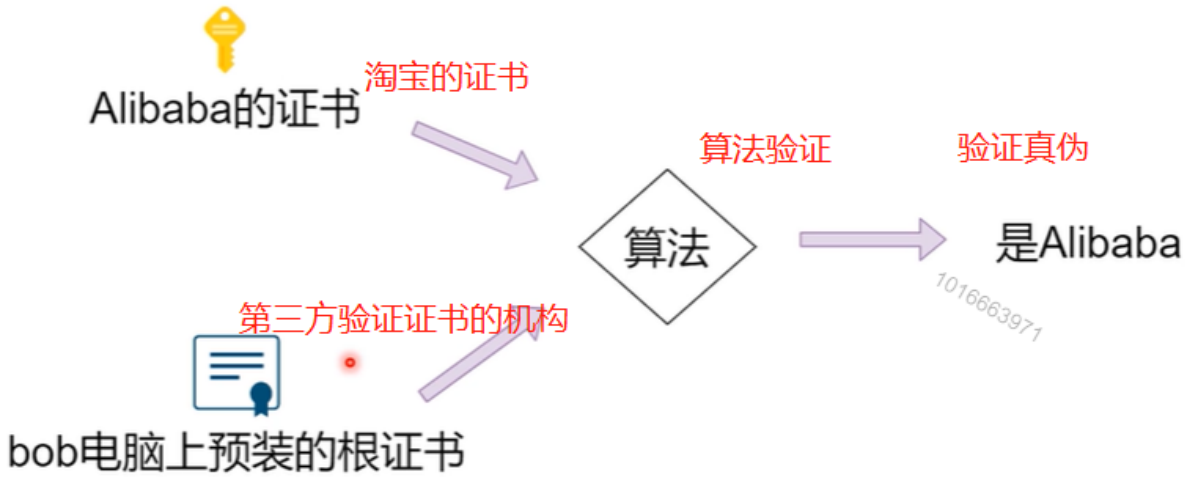
思考，如何解决信任关系?

前面我们说了,公私钥体系的优势，但是有个最核心的没有解决.Bob在浏览器输入网址登录淘宝，打开的是淘宝的首页，Bob是个程序员，心理犯嘀咕，想这到底是真的淘宝，还是我的DNS被劫持了？（DNS劫持指的是，本来应该到淘宝的服务器，结果到了黑客的服务器。黑客把界面做的和淘宝一模一样，让用户信以为真，下单后，付钱没有物流。这是跟以前的钓鱼网站差不多） 这个时候产生一个信任关系。下面就是解决信任关系的。

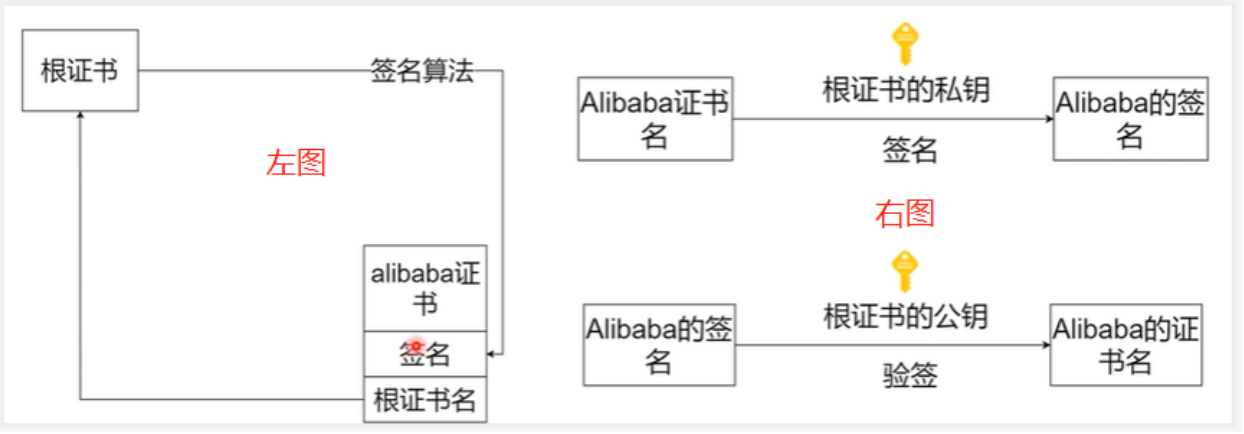


Bob输入淘宝网址，返回淘宝首页，同时返回alibaba含公钥的证书。但是这个证书的真假有待证实?这时候需要第三方去验证这个证书的真假。这里牵扯到一个证书体系了。

证书体系

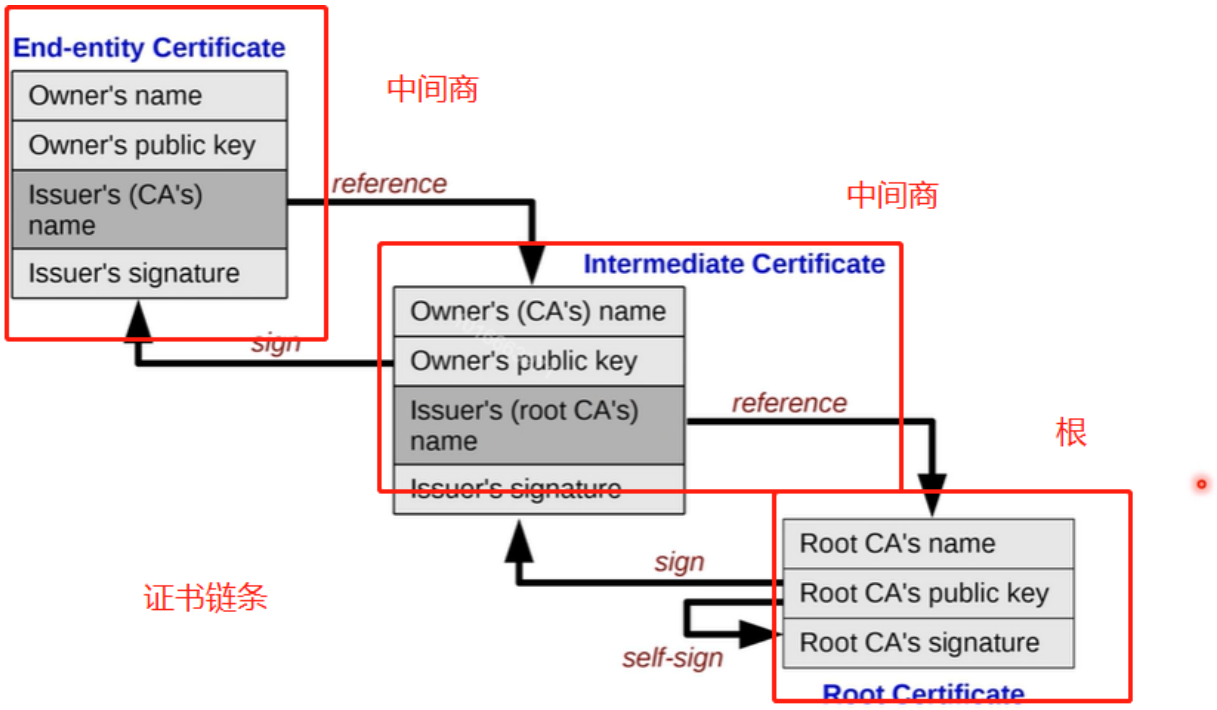


算法如何验证证书



这个算法分成两个部分，比如:阿里巴巴去的能够颁发证书的权威机构，申请一个证书(左图)，根证书签名算法帮阿里巴巴签名，拥有签名后，就产生了阿里巴巴的证书。（右图)这个阿里巴巴的证书是根证书它通过(阿里巴巴提供的私钥)签名的，就变成了阿里巴巴的签名(加密)，Bob拿到阿里巴巴的签名后，通过根证书的公钥去验证(解密)，解密成功，就说明是阿里巴巴的证书，反之则不是。

实际的证书体系



常见算法介绍

- DES(Data Encryption Standard) 1970 IMB提出的对称加密算法 可暴力破解 不太安全

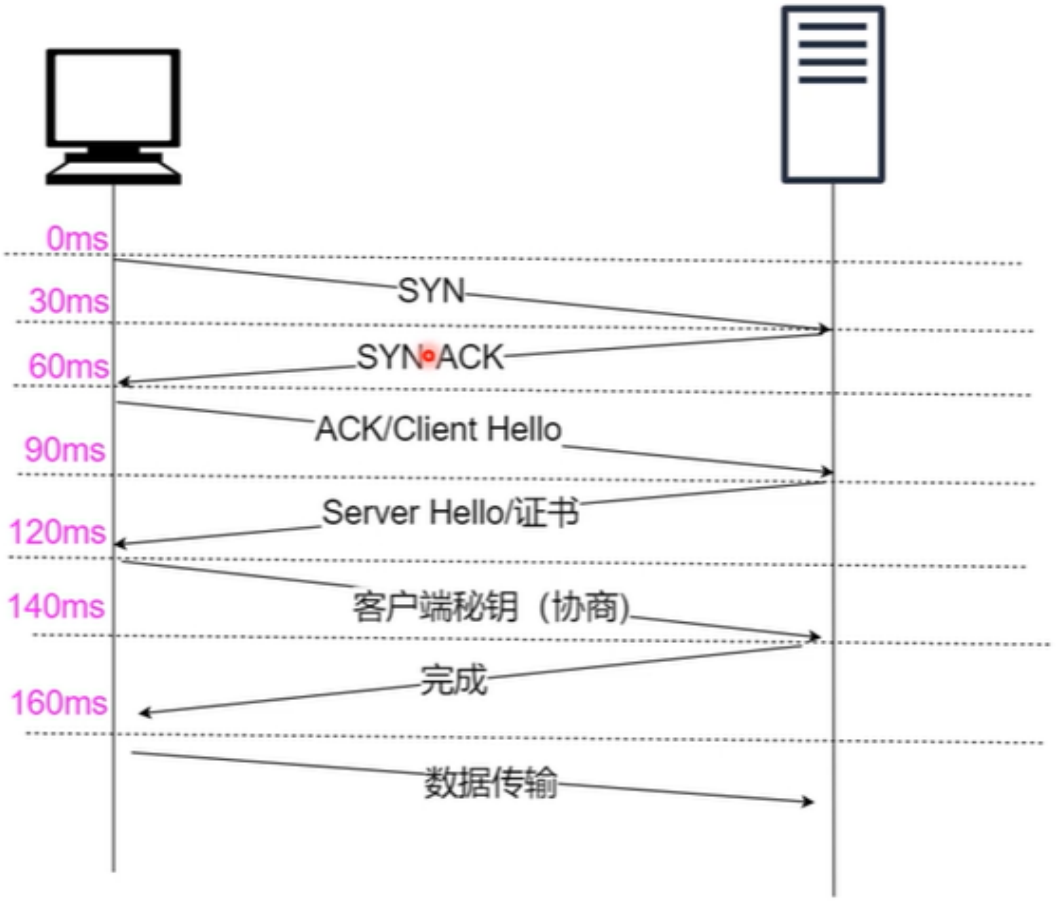
- AES(Advanced Encryption Standard) 2001美国发布的对称加密算法 可旁道攻击
- RSA 1977发布的非对称加密算法

对称vs非对称

- 非对称加密安全性更高
- 对称加密算法速度更快
- 通常混合使用(利用非对称加密协商秘钥，然后进行对称加密)

HTTPS工作原理

https建立连接到工作的过程



1. 建立连接三次握手，SYN---SYN ACK---ACK/Client Hello(未加密)
2. 服务端发Server Hello/证书到客户端(未加密)
3. 客户端秘钥(协商)-使用非对称加密算法协商秘钥(加密)
4. 协商完成后，对称加密算法进行数据传输(加密)

课程小结

加密/解密核心是要解决诚信问题

（凡是能解决诚信问题的方法都可以替代现在的体系）