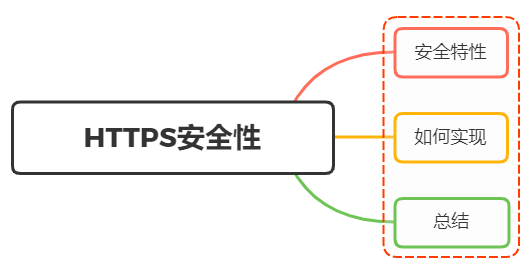
# 面试官：为什么说HTTPS比HTTP安全? HTTPS是如何保证安全的？



## 一、安全特性

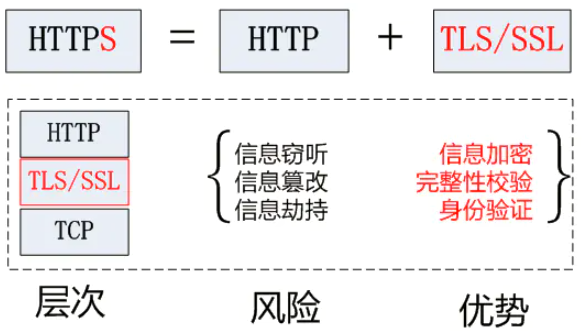
在上篇文章中，我们了解到HTTP在通信过程中，存在以下问题：

* 通信使用明文（不加密），内容可能被窃听
* 不验证通信方的身份，因此有可能遭遇伪装

而HTTPS的出现正是解决这些问题，HTTPS是建立在SSL之上，其安全性由SSL来保证

在采用SSL后，HTTP就拥有了HTTPS的加密、证书和完整性保护这些功能

SSL(Secure Sockets Layer 安全套接字协议),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议



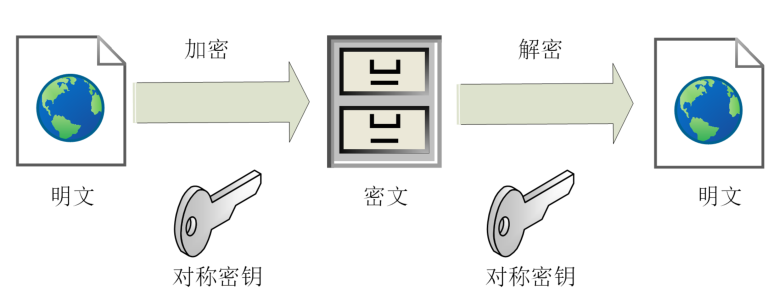
## 二、如何做

SSL的实现这些功能主要依赖于三种手段：

* 对称加密：采用协商的密钥对数据加密
* 非对称加密：实现身份认证和密钥协商
* 摘要算法：验证信息的完整性
* 数字签名：身份验证

### 对称加密

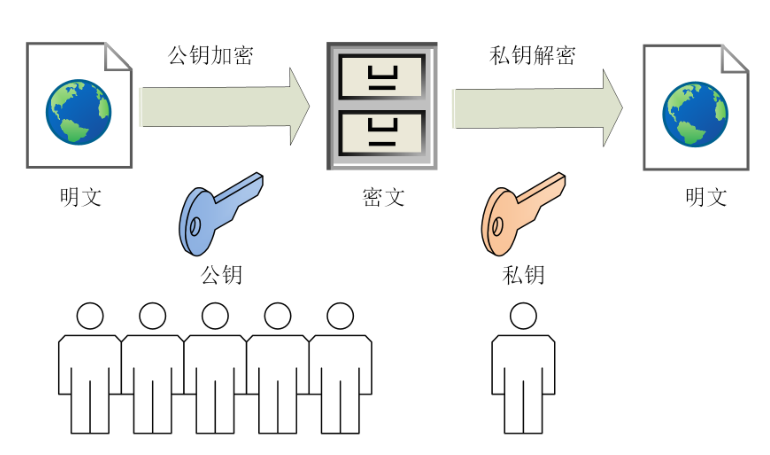
对称加密指的是加密和解密使用的秘钥都是同一个，是对称的。只要保证了密钥的安全，那整个通信过程就可以说具有了机密性



### 非对称加密

非对称加密，存在两个秘钥，一个叫公钥，一个叫私钥。两个秘钥是不同的，公钥可以公开给任何人使用，私钥则需要保密

公钥和私钥都可以用来加密解密，但公钥加密后只能用私钥解 密，反过来，私钥加密后也只能用公钥解密



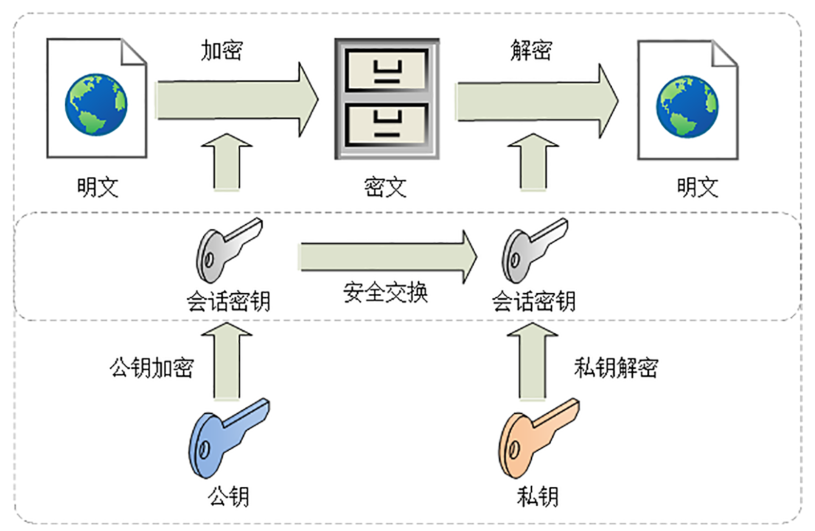
### 混合加密

在HTTPS通信过程中，采用的是对称加密+非对称加密，也就是混合加密

在对称加密中讲到，如果能够保证了密钥的安全，那整个通信过程就可以说具有了机密性

而HTTPS采用非对称加密解决秘钥交换的问题

具体做法是发送密文的一方使用对方的公钥进行加密处理“对称的密钥”，然后对方用自己的私钥解密拿到“对称的密钥”



这样可以确保交换的密钥是安全的前提下，使用对称加密方式进行通信

#### 举个例子：

网站秘密保管私钥，在网上任意分发公钥，你想要登录网站只要用公钥加密就行了，密文只能由私钥持有者才能解密。而黑客因为没有私钥，所以就无法破解密文

上述的方法解决了数据加密，在网络传输过程中，数据有可能被篡改，并且黑客可以伪造身份发布公钥，如果你获取到假的公钥，那么混合加密也并无多大用处，你的数据扔被黑客解决

因此，在上述加密的基础上仍需加上完整性、身份验证的特性，来实现真正的安全，实现这一功能则是摘要算法

### 摘要算法

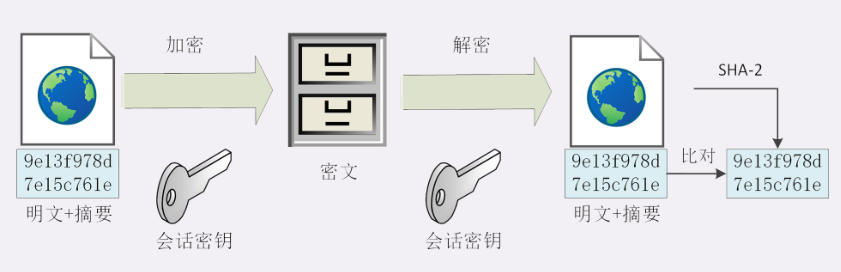
实现完整性的手段主要是摘要算法，也就是常说的散列函数、哈希函数

可以理解成一种特殊的压缩算法，它能够把任意长度的数据“压缩”成固定长度、而且独一无二的“摘要”字符串，就好像是给这段数据生成了一个数字“指纹”



摘要算法保证了“数字摘要”和原文是完全等价的。所以，我们只要在原文后附上它的摘要，就能够保证数据的完整性

比如，你发了条消息：“转账 1000 元”，然后再加上一个 SHA-2 的摘要。网站收到后也计算一下消息的摘要，把这两份“指纹”做个对比，如果一致，就说明消息是完整可信的，没有被修改

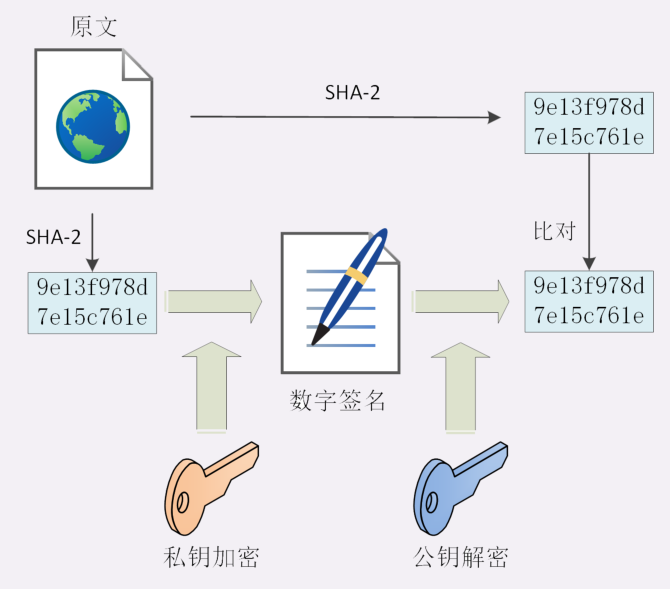


### 数字签名

数字签名能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名

原理其实很简单，就是用私钥加密，公钥解密

签名和公钥一样完全公开，任何人都可以获取。但这个签名只有用私钥对应的公钥才能解开，拿到摘要后，再比对原文验证完整性，就可以像签署文件一样证明消息确实是你发的



和消息本身一样，因为谁都可以发布公钥，我们还缺少防止黑客伪造公钥的手段，也就是说，怎么判断这个公钥就是你的公钥

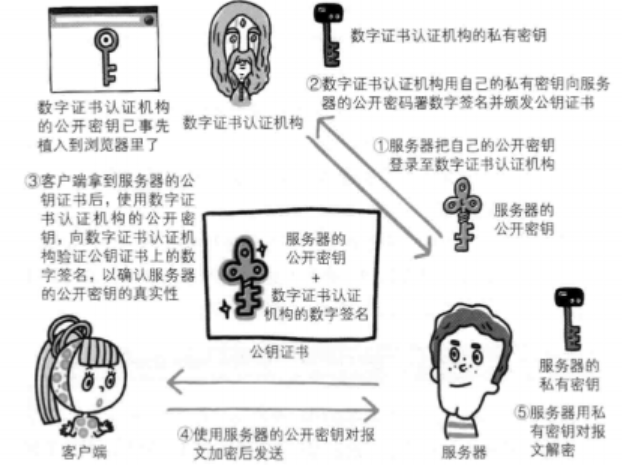
这时候就需要一个第三方，就是证书验证机构

### CA验证机构

数字证书认证机构处于客户端与服务器双方都可信赖的第三方机构的立场

CA 对公钥的签名认证要求包括序列号、用途、颁发者、有效时间等等，把这些打成一个包再签名，完整地证明公钥关联的各种信息，形成“数字证书”

流程如下图：



* 服务器的运营人员向数字证书认证机构提出公开密钥的申请
* 数字证书认证机构在判明提出申请者的身份之后，会对已申请的公开密钥做数字签名
* 然后分配这个已签名的公开密钥，并将该公开密钥放入公钥证书后绑定在一起
* 服务器会将这份由数字证书认证机构颁发的数字证书发送给客户端，以进行非对称加密方式通信

接到证书的客户端可使用数字证书认证机构的公开密钥，对那张证书上的数字签名进行验证，一旦验证通过，则证明：

* 认证服务器的公开密钥的是真实有效的数字证书认证机构
* 服务器的公开密钥是值得信赖的

## 三、总结

可以看到，HTTPS与HTTP虽然只差一个SSL，但是通信安全得到了大大的保障，通信的四大特性都以解决，解决方式如下：

* 机密性：混合算法
* 完整性：摘要算法
* 身份认证：数字签名
* 不可否定：数字签名

同时引入第三方证书机构，确保公开秘钥的安全性

## 参考文献

* https://zhuanlan.zhihu.com/p/100657391
* https://juejin.cn/post/6844903830987997197#heading-7
* https://cloud.tencent.com/developer/article/1748862